

**ROBINSON CALCAGNIE, INC.**

Daniel S. Robinson (SBN 244245)  
*drobinson@robinsonfirm.com*  
Michael W. Olson (SBN 312857)  
*molson@robinsonfirm.com*  
19 Corporate Plaza Drive  
Newport Beach, California  
(949) 720-1288; Fax: (949) 720-1292

**AHDOOT & WOLFSON, PC**

Tina Wolfson (SBN 174806)  
*twolfson@ahdootwolfson.com*  
Alyssa Brown (SBN 301313)  
*abrown@ahdootwolfson.com*  
2600 W. Olive Avenue, Suite 500  
Burbank, California 91505  
(310) 474-9111; Fax: (310) 474-8585

**KAZEROUNI LAW GROUP, APC**

Abbas Kazerounian (SBN 249203)  
*ak@kazlg.com*  
Mona Amini (SBN 296829)  
*mona@kazlg.com*  
245 Fischer Avenue, Suite D1  
Costa Mesa, California 92626  
(800) 400-6808; Fax: (800) 520-5523

*Interim Co-Lead Counsel for Plaintiffs*

**LARSON LLP**

Stephen G. Larson (SBN 145225)  
*slarson@larsonllp.com*  
555 S. Flower Street, 30<sup>th</sup> Floor  
Los Angeles, CA 90071  
(213) 436-4864; Fax: (213) 623-2000

**MILBERG COLEMAN BRYSON  
PHILLIPS GROSSMAN, PLLC**

Gary M. Klinger (*Pro Hac Pending*)  
*gklinger@milberg.com*  
227 W. Monroe Street, Suite 2100  
Chicago, IL 60606  
(866) 252-0878

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA, SOUTHERN DIVISION

*In re loanDepot Data Breach Litigation*

Case No. 8:24-cv-00136-DOC-JDEx

This Document Relates to: All Cases

Assigned For All Purposes to  
Courtroom 10A: Hon. David O. Carter

**CONSOLIDATED CLASS ACTION  
COMPLAINT**

**DEMAND FOR JURY TRIAL**

1 Plaintiffs Alphonso Woods, David Ware, Deborah McPhail, Josh Krieghauser,  
2 Daroya Isaiah, Joshua Beller, Maurice Beckwith, Robert Lash, Ryan Azinger, Lorenz  
3 Praefcke, Varun Singh, Debra Coe, Loretta Montgomery, Vidal Hernandez, Tracy  
4 Brown, Branislav Sasic, Jessica Schuler, Kyle Nunnely, Nailah Ricco-Brown, and  
5 Matthew McFall, individually and on behalf of all others similarly situated,  
6 (collectively, “Plaintiffs”) bring this Consolidated Class Action Complaint and allege  
7 the following against Defendant loanDepot, Inc. (“loanDepot” or “Defendant”), based  
8 upon personal knowledge as to their own acts and investigations, the investigation of  
9 counsel, and information and belief.

## 10 **I. INTRODUCTION**

11 1. This case is about loanDepot’s failure to adequately secure and safeguard  
12 its vulnerable networks, resulting in a massive data breach where the personally  
13 identifiable information of approximately 16.9 million<sup>1</sup> of its nationwide customers  
14 was allegedly accessed and exfiltrated by unauthorized parties. According to  
15 loanDepot’s announcement made on or around January 8, 2024, between January 3-  
16 5, 2024, an unauthorized third party gained access to loanDepot’s systems, including  
17 certain sensitive personal information stored in those systems (the “Data Breach”).  
18 The personal information included Plaintiffs’ and putative class members’ names,  
19 addresses, email addresses, financial account numbers, Social Security numbers  
20 (“SSN”), phone numbers, and dates of birth (collectively, “Private Information”).

21 2. As a result of Defendant’s failure to implement expected and industry-  
22 standard data security practices, Plaintiffs and members of the proposed classes  
23 (defined below) (collectively, the “Class Members”) suffered foreseeable,  
24 preventable, and ascertainable losses.

25 //

26  
27 <sup>1</sup> Office of the Maine Attorney General,  
28 <https://apps.web.maine.gov/online/aewviewer/ME/40/2b910ff6-9bd0-4fcf-a766-cd2c0bc85dec.shtml> (last visited May 9, 2024).

1           3.     loanDepot is an Irvine, California-based nonbank holding company and  
2 the nation's fifth largest retail mortgage lender, funding more than 27,000 consumer  
3 mortgages per month.<sup>2</sup>

4           4.     loanDepot was on notice that it was vulnerable to a cyberattack. Not only  
5 is it industry-wide knowledge that financial institutions experience a consistent stream  
6 of cyberattacks, but loanDepot itself just recently suffered a similar data breach that  
7 exposed its customers' Private Information. In August 2022, third parties hacked into  
8 loanDepot's inadequately secured systems and stole thousands of customers' Private  
9 Information. In that instance, nine months passed until loanDepot even notified its  
10 customers that their Private Information had been stolen, including names and other  
11 personal identifiers in combination with SSNs.<sup>3</sup> Despite knowing of its susceptibility  
12 to a targeted cyberattack and knowing the consequences that would result to  
13 consumers, loanDepot turned a blind eye, failing to implement adequate safeguards  
14 to protect its customers' confidential Private Information.

15           5.     On January 8, 2024, loanDepot announced that once again data thieves  
16 had targeted and gained unauthorized access to its systems and compromised the  
17 Private Information of approximately 16.6 million individuals.<sup>4</sup> That same day,  
18 loanDepot reported in its mandatory U.S. Securities and Exchange Commission  
19 ("SEC") disclosure that hackers had breached its systems.<sup>5</sup>

20           6.     Because of the severity of the Data Breach at issue, on or about January  
21

22 <sup>2</sup> *About Us*, loanDepot, <https://loandepot.com/about> (last visited May 1, 2024).

23 <sup>3</sup> *See* <https://apps.web.maine.gov/online/aewviewer/ME/40/60385809-5ea7-44e0-93a5-4ee98fb42e1e.shtml> (last visited May 9, 2024).

24 <sup>4</sup> *loanDepot Provides Update on Cyber Incident*, loanDepot (Jan. 22, 2024),  
25 <https://investors.loandepot.com/news/corporate-and-financial-news/corporate-and-financial-news-details/2024/loanDepot-Provides-Update-on-Cyber-Incident/default.aspx> (last visited June 3, 2024).

26 <sup>5</sup> *See* loanDepot Form 8-K Filing, <https://d18rn0p25nwr6d.cloudfront.net/CIK-0001831631/446c437f-153f-425d-adc6-bf37155d6e91.pdf> (last visited May 30, 2024).  
28

1 8, 2024, loanDepot shut down its website, including its customer portals.<sup>6</sup>

2 7. loanDepot’s customer service portal, “mellohomes.com” website,  
3 HELOC customer portal, and “myloandepot” customer portal were all down and  
4 inaccessible until January 18, 2024.

5 8. Considering the severity of the Data Breach, the steps that loanDepot has  
6 taken have been insufficient and perfunctory.

7 9. After keeping its customers largely in the dark for two weeks, on January  
8 22, 2024, loanDepot issued the following press release regarding the Data Breach:

9 loanDepot, Inc. (“LDI” or “Company”) (NYSE: LDI), a leading  
10 provider of home lending solutions, today provided an update on the  
11 cyber incident it disclosed on January 8, 2024. The Company has been  
12 working diligently with outside forensics and security experts to  
13 investigate the incident and restore normal operations as quickly as  
14 possible . . . . Although its investigation is ongoing, the Company has  
15 determined that an unauthorized third party gained access to the  
16 sensitive personal information of approximately 16.6 million  
individuals in its systems. The Company will notify these individuals  
and offer credit monitoring and identity protection services at no cost  
to them.<sup>7</sup>

17 10. The January 22, 2024 “update” provided little new information, other  
18 than informing customers they were eligible for free credit monitoring services. This  
19 offer for free services is both the minimum loanDepot could offer in light of the  
20 magnitude of harm it has caused, and serves as a tacit acknowledgment of the  
21 detrimental and elevated risk that all Class Members now imminently face as a result  
22 of Defendant’s acts and omissions surrounding the Data Breach.

23 11. In this update, Defendant’s CEO Frank Martel acknowledged: “we live  
24 in a world where these types of attacks are increasingly frequent and sophisticated,  
25

26 <sup>6</sup> Zack Whittaker, *LoanDepot hit by suspected ransomware attack*, TECHCRUNCH  
27 (Jan. 8, 2024, 10:00 a.m. PST), <https://techcrunch.com/2024/01/08/loandepot-outage-suspected-ransomware-attack/> (last visited June 3, 2024).

28 <sup>7</sup> See, *supra*, n. 4.

1 and our industry has not been spared. We sincerely regret any impact on our  
2 customers.”<sup>8</sup> This message was nothing more than an attempt to deflect responsibility  
3 for loanDepot’s failure to fulfill its legal obligations to protect Plaintiffs’ and Class  
4 Members’ Private Information. The frequency of these types of attacks is exactly why  
5 loanDepot should have taken greater steps to protect Private Information.

6 12. On or about February 23, 2024, almost six weeks after the initial January  
7 8 announcement and SEC filing, Defendant began to provide notice of the Data  
8 Breach to its past, present, or prospective customers, employees, and state attorneys  
9 general.<sup>9</sup> Through these reportings, loanDepot revealed that the number of individuals  
10 affected by this massive Data Breach grew to 16,924,071.

11 13. Through its notice, loanDepot provided that, “[a]s discussed further  
12 below, we recommend you remain vigilant with respect to reviewing your account  
13 statements and credit reports.” loanDepot also provided “Steps You May Take to  
14 Protect Yourself Against Potential Misuse of Information,” which includes reviewing  
15 account statements and periodically pulling a credit report, reviewing fraud alerts, and  
16 obtaining a credit freeze, among other steps that loanDepot recommends Plaintiffs  
17 and Class Members take following the Data Breach.

18 14. Thus, even loanDepot acknowledges the risks associated with the Data  
19 Breach, and that Plaintiffs and Class Members should take immediate steps to protect  
20 themselves from potential harm. loanDepot is, therefore, estopped from contending  
21 Plaintiffs’ and Class Members’ protective actions were unnecessary, unwise, or  
22 unwarranted.

23 15. Despite the threat actors (the ALPHV/BlackCat ransomware gang)  
24 publicly identifying themselves and claiming credit for the Data Breach on February  
25

---

26 <sup>8</sup> See, *supra*, n. 4.

27 <sup>9</sup> Office of the Maine Attorney General,  
28 <https://apps.web.maine.gov/online/aewviewer/ME/40/2b910ff6-9bd0-4fcf-a766-cd2c0bc85dec.shtml> (last visited June 3, 2024).

1 16, 2024, Defendant did not begin to send notices to Plaintiffs, customers, employees,  
 2 and states' attorneys general for another week.<sup>10</sup> The notice did not include critical  
 3 information that the threat actors provided, including that the Russian-linked  
 4 ransomware gang wrote, "Your information is in the final process of being sold.  
 5 That's all."<sup>11</sup> Defendant has failed to provide sufficient details surrounding the Data  
 6 Breach to enable breach victims to arm themselves against fraud and identity theft.

7 16. loanDepot's failure to implement adequate safeguards is particularly  
 8 troublesome considering its assurances that it would safeguard its customers'  
 9 confidential information. Indeed, loanDepot warrants to consumers that it has  
 10 "adopted policies and procedures designed to protect [their] personally identifiable  
 11 information" and that "all data that is considered highly confidential data can only be  
 12 read or written through defined service access points, the use of which is password-  
 13 protected. The physical security of the data is achieved through a combination of  
 14 network firewalls and servers with tested operating systems, all housed in a secure  
 15 facility."<sup>12</sup>

16 17. Relying on these assurances, Plaintiffs and Class Members shared and  
 17 entrusted their Private Information with loanDepot, its officials, and its agents with  
 18 the understanding that—at a minimum—loanDepot would take reasonable steps to  
 19 ensure that this information remained private, safe, and secure from breaches and  
 20 attacks.

21 18. Up to and through January 2024, loanDepot collected, maintained, and  
 22 stored Class Members' Private Information in an unsecured, unencrypted, and  
 23

24 <sup>10</sup> Stefanie Schappert, *LoanDepot finally reveals what data was exposed in Jan*  
 25 *hack*, Cybernews (Feb. 26, 2024, 9:21 p.m.),  
 26 <https://cybernews.com/news/loandepot-finally-reveals-what-data-exposed-in-jan-hack/>.

27 <sup>11</sup> *Id.*

28 <sup>12</sup> *Privacy Policy*, loanDepot, <https://www.loandepot.com/privacypolicy> (last visited May 30, 2024).

1 internet-accessible environment, from which unauthorized actors used an extraction  
2 tool to retrieve sensitive Private Information belonging to Plaintiffs and millions of  
3 Class Members.

4 19. Despite loanDepot's knowledge that its systems were vulnerable to  
5 cyberattacks and its assurances to its customers that it would adequately safeguard  
6 Private Information, Defendant knowingly and willfully maintained Private  
7 Information in a grossly negligent and/or reckless manner by storing that sensitive  
8 information in a condition vulnerable to cyberattacks.

9 20. The severe consequences of exposing Plaintiffs and Class Members'  
10 Private Information to data thieves cannot be exaggerated. Private Information is such  
11 a valuable commodity to identity-thieves that once the information has been  
12 compromised, it is circulated and traded by criminals on the "cyber black-market" for  
13 years.<sup>13</sup> Indeed, as noted above, on February 16, 2024, the threat actors here publicly  
14 announced that the stolen data was in the final process of being sold.<sup>14</sup>

15 21. As a result of the Data Breach and Defendant's untimely notice,  
16 Plaintiffs and Class Members have been exposed to a present, heightened, and  
17 imminent risk of fraud and identity theft. Armed with the Private Information  
18 accessed in the Data Breach, data thieves can commit a variety of crimes including,  
19 but not limited to, opening new financial accounts in Class Members' names, taking  
20 out loans in Class Members' names, using Class Members' names to obtain medical  
21 services, using Class Members' email and telephone information to target Class  
22 Members for other phishing and hacking intrusions, using Class Members'  
23 information to obtain government benefits, filing fraudulent tax returns using Class  
24

25 <sup>13</sup> *PERSONAL INFORMATION: Data Breaches Are Frequent, but Evidence of*  
26 *Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, U.S.  
27 Government Accountability Office, GAO-07-737 (June 2007), at p. 29,  
<https://www.gao.gov/new.items/d07737.pdf>.

28 <sup>14</sup> *See, supra*, n. 10.



1 Members' information, obtaining driver's licenses in Class Members' names, and  
2 more.

3 22. Because of Defendant's willful conduct, Plaintiffs and Class Members  
4 have been required and will be required to continue to undertake time-consuming and  
5 often costly efforts to mitigate the actual and potential harm caused by the Data  
6 Breach. This includes efforts to mitigate the breach's exposure of their Private  
7 Information, including by, among other things, placing freezes and setting alerts with  
8 credit reporting agencies, contacting financial institutions, closing or modifying  
9 financial accounts, reviewing and monitoring credit reports and accounts for  
10 unauthorized activity, changing passwords on potentially impacted websites and  
11 applications, and requesting and maintaining accurate records. This time will be lost  
12 forever and cannot be recaptured.

13 23. Plaintiffs bring this class action on behalf and as representatives of all  
14 similarly situated persons whose personal information was compromised by the Data  
15 Breach. Plaintiffs seek damages and declaratory and injunctive relief to remediate  
16 loanDepot's inadequate data security procedures and practices.

## 17 **II. PARTIES**

### 18 **A. Plaintiffs**

#### 19 **Josh Krieghauser**

20 24. Plaintiff Josh Krieghauser is a resident and citizen of Descanso,  
21 California. Mr. Krieghauser is a customer of loanDepot and applied for and/or  
22 obtained a loan from loanDepot. As a condition of applying for the loan, loanDepot  
23 required Mr. Krieghauser to provide his Private Information to loanDepot in order to  
24 utilize its services. Prior to applying for and/or securing the loan, Mr. Krieghauser  
25 received and reviewed a contract and other documents from loanDepot, which  
26 included and/or incorporated by reference loanDepot's Privacy Policy, which he  
27 reviewed and relied on prior to providing his Private Information to loanDepot. In  
28 providing his Private Information to loanDepot, Mr. Krieghauser reasonably expected



1 loanDepot would maintain the privacy and security of his Private Information, and  
2 would use reasonable measures to protect it in accordance with loanDepot's internal  
3 policies, as well as state and federal law. Mr. Krieghauser reasonably understood that  
4 a portion of the funds paid to loanDepot would be used to pay for adequate data  
5 security and protection of his Private Information. Had Mr. Krieghauser known about  
6 loanDepot's inadequate data security, he would not have provided his Private  
7 Information to loanDepot and/or would have applied for and/or obtained a mortgage  
8 loan through another service provider.

9       25. Mr. Krieghauser is careful about sharing his sensitive Private  
10 Information. Mr. Krieghauser first learned of the Data Breach after receiving a data  
11 breach notification letter dated February 23, 2024, from loanDepot, notifying him of  
12 the Data Breach and that his Private Information had been improperly accessed and  
13 acquired by unauthorized third parties. Upon receiving notice of the Data Breach, Mr.  
14 Krieghauser made reasonable efforts to mitigate the impact thereof, including, but not  
15 limited to, purchasing an identity theft prevention service and frequently monitoring  
16 his various accounts. In the time following the Data Breach, Mr. Krieghauser has  
17 experienced a significant increase in spam phone calls. Mr. Krieghauser has and is  
18 additionally experiencing fear, stress, and frustration because loanDepot disclosed his  
19 Private Information to unauthorized parties who may now use that information for  
20 unknown purposes. Mr. Krieghauser suffered actual injuries in the form of damages  
21 to and diminution in the value of his Private Information—a form of intangible  
22 property entrusted to loanDepot, which was compromised in and as a proximate result  
23 of the Data Breach. Mr. Krieghauser has suffered and will continue to suffer for the  
24 remainder of his life imminent and impending injury arising from the substantially  
25 increased risk of fraud, identity theft, and misuse proximately resulting from his  
26 Private Information being obtained by unauthorized third parties and/or  
27 cybercriminals.

28       26. Mr. Krieghauser has a continuing interest in ensuring that his Private

1 Information, which remains within loanDepot's possession and control, is protected  
2 and safeguarded against future data breaches and cybersecurity risks. The delayed  
3 notification provided by loanDepot further impacted Mr. Krieghauser because it  
4 prevented him from having the earliest opportunity to guard himself against the Data  
5 Breach's harmful effects.

6 **Varun Singh**

7 27. Plaintiff Varun Singh is a resident and citizen of Newark, California. Mr.  
8 Singh is a customer of loanDepot and applied for and/or obtained a loan from  
9 loanDepot in or around November 17, 2020. As a condition of applying for the loan,  
10 loanDepot required Mr. Singh to provide his Private Information to loanDepot in  
11 order to utilize its services. Prior to applying for and/or securing the loan, Mr. Singh  
12 received and reviewed a contract and other documents from loanDepot, which  
13 included and/or incorporated by reference loanDepot's Privacy Policy, which he  
14 reviewed and relied on prior to providing his Private Information to loanDepot. In  
15 providing his Private Information to loanDepot, Mr. Singh reasonably expected  
16 loanDepot would maintain the privacy and security of his Private Information, and  
17 would use reasonable measures to protect it in accordance with loanDepot's internal  
18 policies, as well as state and federal law. Mr. Singh reasonably understood that a  
19 portion of the funds paid to loanDepot would be used to pay for adequate data security  
20 and protection of his Private Information. Had Mr. Singh known about loanDepot's  
21 inadequate data security, he would not have provided his Private Information to  
22 loanDepot and/or would have applied for and/or obtained a mortgage loan through  
23 another service provider.

24 28. Mr. Singh is careful about sharing his sensitive Private Information. Mr.  
25 Singh first learned of the Data Breach after receiving a data breach notification letter  
26 in March 2024, from loanDepot, notifying him of the Data Breach and that his Private  
27 Information, including his social security number, had been improperly accessed and  
28 acquired by unauthorized third parties. Upon receiving notice of the Data Breach, Mr.

1 Singh made reasonable efforts to mitigate the impact thereof, including, but not  
2 limited to, placing a credit freeze and resetting passwords to his various accounts. In  
3 the time following the Data Breach, Mr. Singh has experienced unauthorized attempts  
4 to access his accounts, and he has received calls from anonymous numbers trying to  
5 open accounts using his social security number. Mr. Singh has and is additionally  
6 experiencing fear, stress, and frustration because loanDepot disclosed his Private  
7 Information to unauthorized parties who may now use that information for unknown  
8 purposes. Mr. Singh suffered actual injuries in the form of damages to and diminution  
9 in the value of his Private Information—a form of intangible property entrusted to  
10 loanDepot, which was compromised in and as a proximate result of the Data Breach.  
11 Mr. Singh has suffered and will continue to suffer for the remainder of his life  
12 imminent and impending injury arising from the substantially increased risk of fraud,  
13 identity theft, and misuse proximately resulting from his Private Information being  
14 obtained by unauthorized third parties and/or cybercriminals.

15 29. Mr. Singh has a continuing interest in ensuring that his Private  
16 Information, which remains within loanDepot's possession and control, is protected  
17 and safeguarded against future data breaches and cybersecurity risks. The delayed  
18 notification provided by loanDepot further impacted Mr. Singh because it prevented  
19 him from having the earliest opportunity to guard himself against the Data Breach's  
20 harmful effects.

21 **Daroya Isaiah**

22 30. Plaintiff Daroya Isaiah is a resident and citizen of Adelanto, California.  
23 Ms. Isaiah was a customer of loanDepot and applied for and/or obtained a loan from  
24 loanDepot. As a condition of applying for the loan, loanDepot required Ms. Isaiah to  
25 provide her Private Information to loanDepot in order to utilize its services. Prior to  
26 applying for the loan, Ms. Isaiah received and reviewed a contract and other  
27 documents from loanDepot, which included and/or incorporated by reference  
28 loanDepot's Privacy Policy, which she reviewed and relied on prior to providing her

1 Private Information to loanDepot. In providing her Private Information to loanDepot,  
2 Ms. Isaiah reasonably expected loanDepot would maintain the privacy and security  
3 of her Private Information, and would use reasonable measures to protect it in  
4 accordance with loanDepot's internal policies, as well as state and federal law. Ms.  
5 Isaiah reasonably understood that a portion of the funds that she would have paid to  
6 loanDepot would be used to pay for adequate data security and protection of her  
7 Private Information. Had Ms. Isaiah known about loanDepot's inadequate data  
8 security, she would not have provided her Private Information to loanDepot.

9       31. Ms. Isaiah is careful about sharing her sensitive Private Information. Ms.  
10 Isaiah first learned of the Data Breach after receiving a data breach notification letter  
11 from loanDepot, notifying her of the Data Breach and that her Private Information  
12 had been improperly accessed and acquired by unauthorized third parties. Upon  
13 receiving notice of the Data Breach, Ms. Isaiah made reasonable efforts to mitigate  
14 the impact thereof, including, but not limited to, spending time monitoring her various  
15 accounts, disputing unauthorized charges, freezing her credit, and purchasing credit  
16 reports. In the time following the Data Breach, Ms. Isaiah has experienced  
17 unauthorized fraudulent charges, including an unauthorized fraudulent attempt to  
18 receive governmental student aid in her name. Ms. Isaiah has and is continuing to  
19 experience fear, stress, frustration, and anxiety, among other issues, because  
20 loanDepot disclosed her Private Information to unauthorized parties who may now  
21 use that information for unknown purposes, and any unauthorized activity could have  
22 affected her approval during the homebuying process. Ms. Isaiah suffered actual  
23 injuries in the form of damages to and diminution in the value of her Private  
24 Information—a form of intangible property entrusted to loanDepot, which was  
25 compromised in and as a proximate result of the Data Breach. Ms. Isaiah has suffered  
26 and will continue to suffer for the remainder of her life imminent and impending  
27 injury arising from the substantially increased risk of fraud, identity theft, and misuse  
28 proximately resulting from her Private Information being obtained by unauthorized

1 third parties and/or cybercriminals.

2 32. Ms. Isaiah has a continuing interest in ensuring that her Private  
3 Information, which remains within loanDepot's possession and control, is protected  
4 and safeguarded against future data breaches and cybersecurity risks. The delayed  
5 notification provided by loanDepot further impacted Ms. Isaiah because it prevented  
6 her from having the earliest opportunity to guard herself against the Data Breach's  
7 harmful effects and she would have sooner been able to seek a mortgage loan through  
8 another service provider at a better interest rate.

9 **Alphonso Woods**

10 33. Plaintiff Alphonso Woods is a resident and citizen of Valley Grande,  
11 Alabama. Alphonso Woods is a customer of loanDepot and applied for and/or  
12 obtained a loan from loanDepot. As a condition of applying for the loan, loanDepot  
13 required Mr. Woods to provide his Private Information to loanDepot in order to utilize  
14 its services. Prior to applying for and/or securing the loan, Mr. Woods received and  
15 reviewed a contract and other documents from loanDepot, which included and/or  
16 incorporated by reference loanDepot's Privacy Policy, which he reviewed and relied  
17 on prior to providing his Private Information to loanDepot. In providing his Private  
18 Information to loanDepot, Mr. Woods reasonably expected loanDepot would  
19 maintain the privacy and security of his Private Information, and would use  
20 reasonable measures to protect it in accordance with loanDepot's internal policies, as  
21 well as state and federal law. Mr. Woods reasonably understood that a portion of the  
22 funds paid to loanDepot would be used to pay for adequate data security and  
23 protection of his Private Information. Had Mr. Woods known about loanDepot's  
24 inadequate data security, he would not have provided his Private Information to  
25 loanDepot and/or would have applied for and/or obtained a mortgage loan through  
26 another service provider.

27 34. Mr. Woods is careful about sharing his sensitive Private Information. Mr.  
28 Woods first learned of the Data Breach after receiving a data breach notification letter

1 dated February 2024, from loanDepot, notifying him of the Data Breach and that his  
2 Private Information, including Social Security Number, had been improperly  
3 accessed and acquired by unauthorized third parties. Upon receiving notice of the  
4 Data Breach, Mr. Woods made reasonable efforts to mitigate the impact thereof,  
5 including, but not limited to, freezing his credit and signing up for a monitoring  
6 service. In the time following the Data Breach, Mr. Woods has experienced a  
7 significant increase in spam calls, texts, and emails. Mr. Woods has and is additionally  
8 experiencing fear, stress, and frustration because loanDepot disclosed his Private  
9 Information to unauthorized parties who may now use that information for unknown  
10 purposes. Mr. Woods suffered actual injuries in the form of damages to and  
11 diminution in the value of his Private Information—a form of intangible property  
12 entrusted to loanDepot, which was compromised in and as a proximate result of the  
13 Data Breach. Mr. Woods has suffered and will continue to suffer for the remainder of  
14 his life imminent and impending injury arising from the substantially increased risk  
15 of fraud, identity theft, and misuse proximately resulting from his Private Information  
16 being obtained by unauthorized third parties and/or cybercriminals.

17 35. Mr. Woods has a continuing interest in ensuring that his Private  
18 Information, which remains within loanDepot's possession and control, is protected  
19 and safeguarded against future data breaches and cybersecurity risks. The delayed  
20 notification provided by loanDepot further impacted Mr. Woods because it prevented  
21 him from having the earliest opportunity to guard himself against the Data Breach's  
22 harmful effects.

23 **David Ware**

24 36. Plaintiff David Ware is a resident and citizen of Phoenix, Arizona. Mr.  
25 Ware is a customer of loanDepot and applied for and/or obtained a loan from  
26 loanDepot on or around June 2021. As a condition of applying for the loan, loanDepot  
27 required Mr. Ware to provide his Private Information to loanDepot in order to utilize  
28 its services. Prior to applying for and/or securing the loan, Mr. Ware received and

1 reviewed a contract and other documents from loanDepot, which included and/or  
2 incorporated by reference loanDepot's Privacy Policy, which he reviewed and relied  
3 on prior to providing his Private Information to loanDepot. In providing his Private  
4 Information to loanDepot, Mr. Ware reasonably expected loanDepot would maintain  
5 the privacy and security of his Private Information, and would use reasonable  
6 measures to protect it in accordance with loanDepot's internal policies, as well as state  
7 and federal law. Mr. Ware reasonably understood that a portion of the funds paid to  
8 loanDepot would be used to pay for adequate data security and protection of his  
9 Private Information. Had Mr. Ware known about loanDepot's inadequate data  
10 security, he would not have provided his Private Information to loanDepot and/or  
11 would have applied for and/or obtained a mortgage loan through another service  
12 provider.

13       37. Mr. Ware is careful about sharing his sensitive Private Information. Mr.  
14 Ware first learned of the Data Breach after receiving a data breach notification letter  
15 in or around March 2024, from loanDepot, notifying him of the Data Breach and that  
16 his Private Information had been improperly accessed and acquired by unauthorized  
17 third parties. Upon receiving notice of the Data Breach, Mr. Ware made reasonable  
18 efforts to mitigate the impact thereof, including, but not limited to, subscribing to an  
19 identity theft prevention service and frequently monitoring his online accounts. In the  
20 time following the Data Breach, Mr. Ware has experienced a number of suspicious  
21 emails and unknown individuals opened unauthorized phone accounts using his  
22 information. Mr. Ware has and is additionally experiencing fear, stress, and frustration  
23 because loanDepot disclosed his Private Information to unauthorized parties who may  
24 now use that information for unknown purposes. Mr. Ware suffered actual injuries in  
25 the form of damages to and diminution in the value of his Private Information—a  
26 form of intangible property entrusted to loanDepot, which was compromised in and  
27 as a proximate result of the Data Breach. Mr. Ware has suffered and will continue to  
28 suffer for the remainder of his life imminent and impending injury arising from the



1 substantially increased risk of fraud, identity theft, and misuse proximately resulting  
2 from his Private Information being obtained by unauthorized third parties and/or  
3 cybercriminals.

4 38. Mr. Ware has a continuing interest in ensuring that his Private  
5 Information, which remains within loanDepot's possession and control, is protected  
6 and safeguarded against future data breaches and cybersecurity risks. The delayed  
7 notification provided by loanDepot further impacted Mr. Ware because it prevented  
8 him from having the earliest opportunity to guard himself against the Data Breach's  
9 harmful effects.

10 **Deborah McPhail**

11 39. Plaintiff Deborah McPhail is a resident and citizen of Raymond, Maine.  
12 Ms. McPhail is a customer of loanDepot and applied for and/or obtained a loan from  
13 loanDepot. As a condition of applying for the loan, loanDepot required Ms. McPhail  
14 to provide her Private Information to loanDepot in order to utilize its services. Prior  
15 to applying for and/or securing the loan, Ms. McPhail received and reviewed a  
16 contract and other documents from loanDepot, which included and/or incorporated  
17 by reference loanDepot's Privacy Policy, which she reviewed and relied on prior to  
18 providing her Private Information to loanDepot. In providing her Private Information  
19 to loanDepot, Ms. McPhail reasonably expected loanDepot would maintain the  
20 privacy and security of her Private Information, and would use reasonable measures  
21 to protect it in accordance with loanDepot's internal policies, as well as state and  
22 federal law. Ms. McPhail reasonably understood that a portion of the funds paid to  
23 loanDepot would be used to pay for adequate data security and protection of her  
24 Private Information. Had Ms. McPhail known about loanDepot's inadequate data  
25 security, she would not have provided her Private Information to loanDepot and/or  
26 would have applied for and/or obtained a mortgage loan through another service  
27 provider.

28 //

1           40. Ms. McPhail is careful about sharing her sensitive Private Information.  
2 Ms. McPhail first learned of the Data Breach after receiving a data breach notification  
3 letter from loanDepot, notifying her of the Data Breach and that her Private  
4 Information had been improperly accessed and acquired by unauthorized third parties.  
5 Upon receiving notice of the Data Breach, Ms. McPhail made reasonable efforts to  
6 mitigate the impact thereof, including, but not limited to, purchasing identity theft  
7 protection and spending time monitoring her various accounts. In the time following  
8 the Data Breach, Ms. McPhail has experienced an increase in spam phone calls. Ms.  
9 McPhail has and is additionally experiencing fear, stress, and frustration because  
10 loanDepot disclosed her Private Information to unauthorized parties who may now  
11 use that information for unknown purposes. Ms. McPhail suffered actual injuries in  
12 the form of damages to and diminution in the value of her Private Information—a  
13 form of intangible property entrusted to loanDepot, which was compromised in and  
14 as a proximate result of the Data Breach. Ms. McPhail has suffered and will continue  
15 to suffer for the remainder of her life imminent and impending injury arising from the  
16 substantially increased risk of fraud, identity theft, and misuse proximately resulting  
17 from her Private Information being obtained by unauthorized third parties and/or  
18 cybercriminals.

19           41. Ms. McPhail has a continuing interest in ensuring that her Private  
20 Information, which remains within loanDepot's possession and control, is protected  
21 and safeguarded against future data breaches and cybersecurity risks. The delayed  
22 notification provided by loanDepot further impacted Ms. McPhail because it  
23 prevented her from having the earliest opportunity to guard herself against the Data  
24 Breach's harmful effects.

25           **Joshua Beller**

26           42. Plaintiff Joshua Beller is a resident and citizen of Commerce City,  
27 Colorado. Mr. Beller is a customer of loanDepot and applied for and/or obtained a  
28 loan from loanDepot in or around August 2020. As a condition of applying for the

1 loan, loanDepot required Mr. Beller to provide his Private Information to loanDepot  
2 in order to utilize its services. Prior to applying for and/or securing the loan, Mr. Beller  
3 received and reviewed a contract and other documents from loanDepot, which  
4 included and/or incorporated by reference loanDepot's Privacy Policy, which he  
5 reviewed and relied on prior to providing his Private Information to loanDepot. In  
6 providing his Private Information to loanDepot, Mr. Beller reasonably expected  
7 loanDepot would maintain the privacy and security of his Private Information, and  
8 would use reasonable measures to protect it in accordance with loanDepot's internal  
9 policies, as well as state and federal law. Mr. Beller reasonably understood that a  
10 portion of the funds paid to loanDepot would be used to pay for adequate data security  
11 and protection of his Private Information. Had Mr. Beller known about loanDepot's  
12 inadequate data security, he would not have provided his Private Information to  
13 loanDepot and/or would have applied for and/or obtained a mortgage loan through  
14 another service provider.

15 43. Mr. Beller is careful about sharing his sensitive Private Information. Mr.  
16 Beller first learned of the Data Breach after receiving a data breach notification letter  
17 in or around March 2024, from loanDepot, notifying him of the Data Breach and that  
18 his Private Information had been improperly accessed and acquired by unauthorized  
19 third parties. Upon receiving notice of the Data Breach, Mr. Beller made reasonable  
20 efforts to mitigate the impact thereof, including, but not limited to, purchasing an  
21 identity theft prevention service and spending hours a week monitoring his various  
22 online accounts. In the time following the Data Breach, Mr. Beller has experienced a  
23 significant uptick in spam calls and spam emails. Mr. Beller has and is additionally  
24 experiencing fear, stress, and frustration because loanDepot disclosed his Private  
25 Information to unauthorized parties who may now use that information for unknown  
26 purposes. Mr. Beller suffered actual injuries in the form of damages to and diminution  
27 in the value of his Private Information—a form of intangible property entrusted to  
28 loanDepot, which was compromised in and as a proximate result of the Data Breach.

1 Mr. Beller has suffered and will continue to suffer for the remainder of his life  
2 imminent and impending injury arising from the substantially increased risk of fraud,  
3 identity theft, and misuse proximately resulting from his Private Information being  
4 obtained by unauthorized third parties and/or cybercriminals.

5 44. Mr. Beller has a continuing interest in ensuring that his Private  
6 Information, which remains within loanDepot's possession and control, is protected  
7 and safeguarded against future data breaches and cybersecurity risks. The delayed  
8 notification provided by loanDepot further impacted Mr. Beller because it prevented  
9 him from having the earliest opportunity to guard himself against the Data Breach's  
10 harmful effects.

11 **Maurice Beckwith**

12 45. Plaintiff Maurice Beckwith is a resident and citizen of Durham, North  
13 Carolina. Mr. Beckwith is a customer of loanDepot and applied for and/or obtained  
14 a loan from loanDepot. As a condition of applying for the loan, loanDepot required  
15 Mr. Beckwith to provide his Private Information to loanDepot in order to utilize its  
16 services. Prior to applying for and/or securing the loan, Mr. Beckwith received and  
17 reviewed a contract and other documents from loanDepot, which included and/or  
18 incorporated by reference loanDepot's Privacy Policy, which he reviewed and relied  
19 on prior to providing his Private Information to loanDepot. In providing his Private  
20 Information to loanDepot, Mr. Beckwith reasonably expected loanDepot would  
21 maintain the privacy and security of his Private Information, and would use  
22 reasonable measures to protect it in accordance with loanDepot's internal policies, as  
23 well as state and federal law. Mr. Beckwith reasonably understood that a portion of  
24 the funds paid to loanDepot would be used to pay for adequate data security and  
25 protection of his Private Information. Had Mr. Beckwith known about loanDepot's  
26 inadequate data security, he would not have provided his Private Information to  
27 loanDepot and/or would have applied for and/or obtained a mortgage loan through  
28 another service provider.

1           46. Mr. Beckwith is careful about sharing his sensitive Private Information.  
2 Mr. Beckwith first learned of the Data Breach after receiving a data breach  
3 notification letter dated February 23, 2024, from loanDepot, notifying him of the Data  
4 Breach and that his Private Information had been improperly accessed and acquired  
5 by unauthorized third parties. Upon receiving notice of the Data Breach, Mr.  
6 Beckwith made reasonable efforts to mitigate the impact thereof, including, but not  
7 limited to, obtaining credit monitoring services and freezing his credit. In the time  
8 following the Data Breach, Mr. Beckwith has experienced fraudulent charges,  
9 unauthorized credit cards opened in his name, and an increase in spam calls, texts,  
10 and emails. Mr. Beckwith has and is additionally experiencing fear, stress, and  
11 frustration because loanDepot disclosed his Private Information to unauthorized  
12 parties who may now use that information for unknown purposes. Mr. Beckwith  
13 suffered actual injuries in the form of damages to and diminution in the value of his  
14 Private Information—a form of intangible property entrusted to loanDepot, which  
15 was compromised in and as a proximate result of the Data Breach. Mr. Beckwith has  
16 suffered and will continue to suffer for the remainder of his life imminent and  
17 impending injury arising from the substantially increased risk of fraud, identity theft,  
18 and misuse proximately resulting from his Private Information being obtained by  
19 unauthorized third parties and/or cybercriminals.

20           47. Mr. Beckwith has a continuing interest in ensuring that his Private  
21 Information, which remains within loanDepot's possession and control, is protected  
22 and safeguarded against future data breaches and cybersecurity risks. The delayed  
23 notification provided by loanDepot further impacted Mr. Beckwith because it  
24 prevented him from having the earliest opportunity to guard himself against the Data  
25 Breach's harmful effects.

26           **Robert Lash**

27           48. Plaintiff Robert Lash is a resident and citizen of Montague, Michigan.  
28 Mr. Lash is a customer of loanDepot and applied for and/or obtained a loan from

1 loanDepot around ten years ago. As a condition of applying for the loan, loanDepot  
2 required Mr. Lash to provide his Private Information to loanDepot in order to utilize  
3 its services. Prior to applying for and/or securing the loan, Mr. Lash received and  
4 reviewed a contract and other documents from loanDepot, which included and/or  
5 incorporated by reference loanDepot's Privacy Policy, which he reviewed and relied  
6 on prior to providing his Private Information to loanDepot. In providing his Private  
7 Information to loanDepot, Mr. Lash reasonably expected loanDepot would maintain  
8 the privacy and security of his Private Information, and would use reasonable  
9 measures to protect it in accordance with loanDepot's internal policies, as well as state  
10 and federal law. Mr. Lash reasonably understood that a portion of the funds paid to  
11 loanDepot would be used to pay for adequate data security and protection of his  
12 Private Information. Had Mr. Lash known about loanDepot's inadequate data  
13 security, he would not have provided his Private Information to loanDepot and/or  
14 would have applied for and/or obtained a mortgage loan through another service  
15 provider.

16       49. Mr. Lash is careful about sharing his sensitive Private Information. Mr.  
17 Lash first learned of the Data Breach after receiving a data breach notification letter  
18 dated February 23, 2024, from loanDepot, notifying him of the Data Breach and that  
19 his Private Information had been improperly accessed and acquired by unauthorized  
20 third parties. Upon receiving notice of the Data Breach, Mr. Lash made reasonable  
21 efforts to mitigate the impact thereof, including, but not limited to, signing up for an  
22 identity theft prevention service and freezing his credit. In the time following the Data  
23 Breach, Mr. Lash has experienced attempted fraudulent charges on his bank account  
24 and an increase in spam calls. Mr. Lash has and is additionally experiencing fear,  
25 stress, and frustration because loanDepot disclosed his Private Information to  
26 unauthorized parties who may now use that information for unknown purposes. Mr.  
27 Lash suffered actual injuries in the form of damages to and diminution in the value of  
28 his Private Information—a form of intangible property entrusted to loanDepot, which

1 was compromised in and as a proximate result of the Data Breach. Mr. Lash has  
2 suffered and will continue to suffer for the remainder of his life imminent and  
3 impending injury arising from the substantially increased risk of fraud, identity theft,  
4 and misuse proximately resulting from his Private Information being obtained by  
5 unauthorized third parties and/or cybercriminals.

6 50. Mr. Lash has a continuing interest in ensuring that his Private  
7 Information, which remains within loanDepot's possession and control, is protected  
8 and safeguarded against future data breaches and cybersecurity risks. The delayed  
9 notification provided by loanDepot further impacted Mr. Lash because it prevented  
10 him from having the earliest opportunity to guard himself against the Data Breach's  
11 harmful effects.

12 **Ryan Azinger**

13 51. Plaintiff Ryan Azinger is a resident and citizen of Sudbury,  
14 Massachusetts. Mr. Azinger is a customer of loanDepot and applied for and/or  
15 obtained a loan from loanDepot on or around June 2021. As a condition of applying  
16 for the loan, loanDepot required Mr. Azinger to provide his Private Information to  
17 loanDepot in order to utilize its services. Prior to applying for and/or securing the  
18 loan, Mr. Azinger received and reviewed a contract and other documents from  
19 loanDepot, which included and/or incorporated by reference loanDepot's Privacy  
20 Policy, which he reviewed and relied on prior to providing his Private Information to  
21 loanDepot. In providing his Private Information to loanDepot, Mr. Azinger  
22 reasonably expected loanDepot would maintain the privacy and security of his Private  
23 Information, and would use reasonable measures to protect it in accordance with  
24 loanDepot's internal policies, as well as state and federal law. Mr. Azinger reasonably  
25 understood that a portion of the funds paid to loanDepot would be used to pay for  
26 adequate data security and protection of his Private Information. Had Mr. Azinger  
27 known about loanDepot's inadequate data security, he would not have provided his  
28 Private Information to loanDepot and/or would have applied for and/or obtained a



1 mortgage loan through another service provider.

2       52. Mr. Azinger is careful about sharing his sensitive Private Information.  
3 Mr. Azinger first learned of the Data Breach after receiving a data breach notification  
4 letter in or around late March 2024, from loanDepot, notifying him of the Data Breach  
5 and that his Private Information had been improperly accessed and acquired by  
6 unauthorized third parties. Upon receiving notice of the Data Breach, Mr. Azinger  
7 made reasonable efforts to mitigate the impact thereof, including, but not limited to,  
8 freezing his credit and informing his local financial institutions about the  
9 compromised data. In the time following the Data Breach, Mr. Azinger has  
10 experienced a number of incidents where someone attempted to open credit accounts  
11 in his name. Mr. Azinger has already received notifications that his information was  
12 on the dark web. Mr. Azinger has and is additionally experiencing fear, stress, and  
13 frustration because loanDepot disclosed his Private Information to unauthorized  
14 parties who may now use that information for unknown purposes. Mr. Azinger  
15 suffered actual injuries in the form of damages to and diminution in the value of his  
16 Private Information—a form of intangible property entrusted to loanDepot, which  
17 was compromised in and as a proximate result of the Data Breach. Mr. Azinger has  
18 suffered and will continue to suffer for the remainder of his life imminent and  
19 impending injury arising from the substantially increased risk of fraud, identity theft,  
20 and misuse proximately resulting from his Private Information being obtained by  
21 unauthorized third parties and/or cybercriminals.

22       53. Mr. Azinger has a continuing interest in ensuring that his Private  
23 Information, which remains within loanDepot's possession and control, is protected  
24 and safeguarded against future data breaches and cybersecurity risks. The delayed  
25 notification provided by loanDepot further impacted Mr. Azinger because it  
26 prevented him from having the earliest opportunity to guard himself against the Data  
27 Breach's harmful effects.

28 //

1           **Lorenz Praefcke**

2           54. Plaintiff Lorenz Praefcke is a resident and citizen of Berwyn,  
3 Pennsylvania. Mr. Praefcke is a customer of loanDepot and applied for and/or  
4 obtained a loan from loanDepot on or around June 2021. As a condition of applying  
5 for the loan, loanDepot required Mr. Praefcke to provide his Private Information to  
6 loanDepot in order to utilize its services. Prior to applying for and/or securing the  
7 loan, Mr. Praefcke received and reviewed a contract and other documents from  
8 loanDepot, which included and/or incorporated by reference loanDepot's Privacy  
9 Policy, which he reviewed and relied on prior to providing his Private Information to  
10 loanDepot. In providing his Private Information to loanDepot, Mr. Praefcke  
11 reasonably expected loanDepot would maintain the privacy and security of his Private  
12 Information, and would use reasonable measures to protect it in accordance with  
13 loanDepot's internal policies, as well as state and federal law. Mr. Praefcke  
14 reasonably understood that a portion of the funds paid to loanDepot would be used to  
15 pay for adequate data security and protection of his Private Information. Had Mr.  
16 Praefcke known about loanDepot's inadequate data security, he would not have  
17 provided his Private Information to loanDepot and/or would have applied for and/or  
18 obtained a mortgage loan through another service provider.

19           55. Mr. Praefcke is careful about sharing his sensitive Private Information.  
20 Mr. Praefcke first learned of the Data Breach after receiving a data breach notification  
21 letter dated February 23, 2024, from loanDepot, notifying him of the Data Breach and  
22 that his Private Information had been improperly accessed and acquired by  
23 unauthorized third parties. Upon receiving notice of the Data Breach, Mr. Praefcke  
24 made reasonable efforts to mitigate the impact thereof, including, but not limited to,  
25 having multiple conversations with Chase, securing his account, talking to his bank  
26 to decline additional applications, and freezing his credit with Transunion. In the time  
27 following the Data Breach, but before receiving the notice, Mr. Praefcke experienced  
28 two unauthorized attempts to open credit cards in his name, along with a significant

1 number of spam calls and emails. Mr. Praefcke has and is additionally experiencing  
2 fear, stress, and frustration because loanDepot disclosed his Private Information to  
3 unauthorized parties who may now use that information for unknown purposes. Mr.  
4 Praefcke suffered actual injuries in the form of damages to and diminution in the value  
5 of his Private Information—a form of intangible property entrusted to loanDepot,  
6 which was compromised in and as a proximate result of the Data Breach. Mr. Praefcke  
7 has suffered and will continue to suffer for the remainder of his life imminent and  
8 impending injury arising from the substantially increased risk of fraud, identity theft,  
9 and misuse proximately resulting from his Private Information being obtained by  
10 unauthorized third parties and/or cybercriminals.

11       56. Mr. Praefcke has a continuing interest in ensuring that his Private  
12 Information, which remains within loanDepot's possession and control, is protected  
13 and safeguarded against future data breaches and cybersecurity risks. The delayed  
14 notification provided by loanDepot further impacted Mr. Praefcke because it  
15 prevented him from having the earliest opportunity to guard himself against the Data  
16 Breach's harmful effects.

17       **Debra Coe**

18       57. Plaintiff Debra Coe is a resident and citizen of Northbrook, Illinois. Ms.  
19 Coe is a customer of loanDepot and applied for and/or obtained a loan from loanDepot  
20 in or around 2019. As a condition of applying for the loan, loanDepot required Ms.  
21 Coe to provide her Private Information to loanDepot in order to utilize its services.  
22 Prior to applying for and/or securing the loan, Ms. Coe received and reviewed a  
23 contract and other documents from loanDepot, which included and/or incorporated  
24 by reference loanDepot's Privacy Policy, which she reviewed and relied on prior to  
25 providing her Private Information to loanDepot. In providing her Private Information  
26 to loanDepot, Ms. Coe reasonably expected loanDepot would maintain the privacy  
27 and security of her Private Information, and would use reasonable measures to protect  
28 it in accordance with loanDepot's internal policies, as well as state and federal law.

1 Ms. Coe reasonably understood that a portion of the funds paid to loanDepot would  
2 be used to pay for adequate data security and protection of her Private Information.  
3 Had Ms. Coe known about loanDepot's inadequate data security, she would not have  
4 provided her Private Information to loanDepot and/or would have applied for and/or  
5 obtained a mortgage loan through another service provider.

6 58. Ms. Coe is careful about sharing her sensitive Private Information. Ms.  
7 Coe first learned of the Data Breach after receiving a data breach notification letter  
8 dated February 2024, from loanDepot, notifying her of the Data Breach and that her  
9 Private Information, including her social security number, had been improperly  
10 accessed and acquired by unauthorized third parties. Upon receiving notice of the  
11 Data Breach, Ms. Coe made reasonable efforts to mitigate the impact thereof. In the  
12 time following the Data Breach, Ms. Coe has experienced a significant increase in  
13 spam calls and texts. Ms. Coe has also experienced fear, stress, and frustration because  
14 loanDepot disclosed her Private Information to unauthorized parties who may now  
15 use that information for unknown purposes. Ms. Coe suffered actual injuries in the  
16 form of damages to and diminution in the value of her PII—a form of intangible  
17 property entrusted to loanDepot, which was compromised in and as a proximate result  
18 of the Data Breach. Ms. Coe has suffered and will continue to suffer for the remainder  
19 of her life imminent and impending injury arising from the substantially increased  
20 risk of fraud, identity theft, and misuse proximately resulting from her Private  
21 Information being obtained by unauthorized third parties and/or cybercriminals.

22 59. Ms. Coe has a continuing interest in ensuring that her Private  
23 Information, which remains within loanDepot's possession and control, is protected  
24 and safeguarded against future data breaches and cybersecurity risks. The delayed  
25 notification provided by loanDepot further impacted Ms. Coe because it prevented  
26 her from having the earliest opportunity to guard herself against the Data Breach's  
27 harmful effects.

28 //

1           **Nailah Ricco-Brown**

2           60. Plaintiff Nailah Ricco-Brown is a resident and citizen of New York, New  
3 York. Ms. Ricco-Brown was a customer of loanDepot and applied for a loan from  
4 loanDepot as part of a program in conjunction with the State of New York Mortgage  
5 Agency. As a condition of applying for the loan, loanDepot required Ms. Ricco-  
6 Brown to provide her Private Information to loanDepot in order to utilize its services.  
7 Prior to applying for the loan, Ms. Ricco-Brown received and reviewed a contract and  
8 other documents from loanDepot, which included and/or incorporated by reference  
9 loanDepot's Privacy Policy, which she reviewed and relied on prior to providing her  
10 Private Information to loanDepot. In providing her Private Information to loanDepot,  
11 Ms. Ricco-Brown reasonably expected loanDepot would maintain the privacy and  
12 security of her Private Information, and would use reasonable measures to protect it  
13 in accordance with loanDepot's internal policies, as well as state and federal law. Ms.  
14 Ricco-Brown reasonably understood that a portion of the funds that she would have  
15 paid to loanDepot would be used to pay for adequate data security and protection of  
16 her Private Information. Had Ms. Ricco-Brown known about loanDepot's inadequate  
17 data security, she would not have provided her Private Information to loanDepot.  
18 Upon learning of the Data Breach, she discontinued her applications process with  
19 loanDepot, which delayed her mortgage loan, resulting in her obtaining a mortgage  
20 loan through another service provider at a higher interest rate than she would have  
21 otherwise received.

22           61. Ms. Ricco-Brown is careful about sharing her sensitive Private  
23 Information. Ms. Ricco-Brown first learned of the Data Breach after receiving a data  
24 breach notification letter from loanDepot, notifying her of the Data Breach and that  
25 her Private Information had been improperly accessed and acquired by unauthorized  
26 third parties. Upon receiving notice of the Data Breach, Ms. Ricco-Brown made  
27 reasonable efforts to mitigate the impact thereof, including, but not limited to,  
28 spending time monitoring her various accounts and continuing to pay for credit

1 monitoring. In the time following the Data Breach, Ms. Ricco-Brown has experienced  
2 an increase in spam phone calls and messages, and she received a notification that  
3 someone had sought a personal loan through a lender in her name for which she did  
4 not seek. Ms. Ricco-Brown has and is continuing to experience fear, stress,  
5 frustration, and anxiety, among other issues, because loanDepot disclosed her Private  
6 Information to unauthorized parties who may now use that information for unknown  
7 purposes, and any unauthorized activity could have affected her approval during the  
8 homebuying process. Ms. Ricco-Brown suffered actual injuries in the form of  
9 damages to and diminution in the value of her Private Information—a form of  
10 intangible property entrusted to loanDepot, which was compromised in and as a  
11 proximate result of the Data Breach. Ms. Ricco-Brown has suffered and will continue  
12 to suffer for the remainder of her life imminent and impending injury arising from the  
13 substantially increased risk of fraud, identity theft, and misuse proximately resulting  
14 from her Private Information being obtained by unauthorized third parties and/or  
15 cybercriminals.

16         62. Ms. Ricco-Brown has a continuing interest in ensuring that her Private  
17 Information, which remains within loanDepot's possession and control, is protected  
18 and safeguarded against future data breaches and cybersecurity risks. The delayed  
19 notification provided by loanDepot further impacted Ms. Ricco-Brown because it  
20 prevented her from having the earliest opportunity to guard herself against the Data  
21 Breach's harmful effects and she would have sooner been able to seek a mortgage  
22 loan through another service provider at a better interest rate.

23         **Loretta Montgomery**

24         63. Plaintiff Loretta Montgomery is a resident and citizen of Fremont, Ohio.  
25 Ms. Montgomery does not recall having applied for a loan or refinance through  
26 loanDepot, or otherwise recall having been a loanDepot customer, and does not know  
27 or recall how loanDepot obtained her Private Information. Had Ms. Montgomery  
28 known that loanDepot possessed her Private Information, she would have expected

1 loanDepot to use reasonable measures to protect it in accordance with loanDepot's  
2 internal policies, as well as state and federal law.

3       64. Ms. Montgomery is careful about sharing her sensitive Private  
4 Information. Ms. Montgomery first learned of the Data Breach after receiving a data  
5 breach notification letter dated February 23, 2024, from loanDepot, notifying her of  
6 the Data Breach and that her Private Information, including her social security  
7 number, had been improperly accessed and acquired by unauthorized third parties.  
8 Although she has never been a loanDepot customer and did not know loanDepot  
9 possessed her Private Information, Ms. Montgomery still took the notice seriously,  
10 and made reasonable efforts to mitigate the impact thereof. In the time following the  
11 Data Breach, Ms. Montgomery has experienced an increase in spam calls. Ms.  
12 Montgomery has and is additionally experiencing fear, stress, and frustration because  
13 loanDepot disclosed her Private Information, which she does not recall providing to  
14 loanDepot, to unauthorized parties who may now use that information for unknown  
15 purposes. Ms. Montgomery suffered actual injuries in the form of damages to and  
16 diminution in the value of her Private Information—a form of intangible property  
17 entrusted to loanDepot, which was compromised in and as a proximate result of the  
18 Data Breach. Ms. Montgomery has suffered and will continue to suffer for the  
19 remainder of her life imminent and impending injury arising from the substantially  
20 increased risk of fraud, identity theft, and misuse proximately resulting from her  
21 Private Information being obtained by unauthorized third parties and/or  
22 cybercriminals.

23       65. Ms. Montgomery has a continuing interest in ensuring that her Private  
24 Information, which remains within loanDepot's possession and control, is protected  
25 and safeguarded against future data breaches and cybersecurity risks. The delayed  
26 notification provided by loanDepot further impacted Ms. Montgomery because it  
27 prevented her from having the earliest opportunity to guard herself against the Data  
28 Breach's harmful effects.



1           **Vidal Hernandez**

2           66. Plaintiff Vidal Hernandez is a resident and citizen of Brooklyn, New  
3 York. Mr. Hernandez does not recall having applied for a loan or refinance through  
4 loanDepot, or otherwise recall having been a loanDepot customer, and does not know  
5 or recall how loanDepot obtained his Private Information. Had Mr. Hernandez known  
6 that loanDepot possessed his Private Information, he would have expected loanDepot  
7 to use reasonable measures to protect it in accordance with loanDepot's internal  
8 policies, as well as state and federal law.

9           67. Mr. Hernandez is careful about sharing his sensitive Private Information.  
10 Mr. Hernandez first learned of the Data Breach after receiving a data breach  
11 notification letter in or around March 2024, from loanDepot, notifying him of the Data  
12 Breach and that his Private Information, including his social security number, had  
13 been improperly accessed and acquired by unauthorized third parties. Although he  
14 has never been a loanDepot customer and did not know loanDepot possessed his  
15 Private Information, Mr. Hernandez still took the notice seriously, and made  
16 reasonable efforts to mitigate the impact thereof. In the time following the Data  
17 Breach, Mr. Hernandez has experienced an increase in spam calls, as well as  
18 unauthorized charges on his debit card. Mr. Hernandez has and is additionally  
19 experiencing fear, stress, and frustration because loanDepot disclosed his Private  
20 Information, which he does not recall providing to loanDepot, to unauthorized parties  
21 who may now use that information for unknown purposes. Mr. Hernandez suffered  
22 actual injuries in the form of damages to and diminution in the value of his Private  
23 Information—a form of intangible property entrusted to loanDepot, which was  
24 compromised in and as a proximate result of the Data Breach. Mr. Hernandez has  
25 suffered and will continue to suffer for the remainder of his life imminent and  
26 impending injury arising from the substantially increased risk of fraud, identity theft,  
27 and misuse proximately resulting from his Private Information being obtained by  
28 unauthorized third parties and/or cybercriminals.

1           68. Mr. Hernandez has a continuing interest in ensuring that his Private  
2 Information, which remains within loanDepot's possession and control, is protected  
3 and safeguarded against future data breaches and cybersecurity risks. The delayed  
4 notification provided by loanDepot further impacted Mr. Hernandez because it  
5 prevented him from having the earliest opportunity to guard himself against the Data  
6 Breach's harmful effects.

7           **Tracy Brown**

8           69. Plaintiff Tracy Brown is a resident and citizen of West Memphis,  
9 Arkansas. Mr. Brown does not recall having applied for a loan or refinance through  
10 loanDepot, or otherwise recall having been a loanDepot customer, and does not know  
11 or recall how loanDepot obtained his Private Information. Had Mr. Brown known that  
12 loanDepot possessed his Private Information, he would have expected loanDepot to  
13 use reasonable measures to protect it in accordance with loanDepot's internal policies,  
14 as well as state and federal law.

15           70. Mr. Brown is careful about sharing his sensitive Private Information. Mr.  
16 Brown first learned of the Data Breach after receiving a data breach notification letter,  
17 from loanDepot, notifying him of the Data Breach and that his Private Information,  
18 including his social security number, had been improperly accessed and acquired by  
19 unauthorized third parties. Although he has never been a loanDepot customer and did  
20 not know loanDepot possessed his Private Information, Mr. Brown still took the  
21 notice seriously, and made reasonable efforts to mitigate the impact thereof,  
22 including, but not limited to, purchasing an identity theft prevention service and  
23 freezing his credit. In the time following the Data Breach, Mr. Brown has experienced  
24 an increase in spam calls. Mr. Brown has and is additionally experiencing fear, stress,  
25 and frustration because loanDepot disclosed his Private Information, which he does  
26 not recall providing to loanDepot, to unauthorized parties who may now use that  
27 information for unknown purposes. Mr. Brown suffered actual injuries in the form of  
28 damages to and diminution in the value of his Private Information—a form of

1 intangible property entrusted to loanDepot, which was compromised in and as a  
2 proximate result of the Data Breach. Mr. Brown has suffered and will continue to  
3 suffer for the remainder of his life imminent and impending injury arising from the  
4 substantially increased risk of fraud, identity theft, and misuse proximately resulting  
5 from his Private Information being obtained by unauthorized third parties and/or  
6 cybercriminals.

7       71. Mr. Brown has a continuing interest in ensuring that his Private  
8 Information, which remains within loanDepot's possession and control, is protected  
9 and safeguarded against future data breaches and cybersecurity risks. The delayed  
10 notification provided by loanDepot further impacted Mr. Brown because it prevented  
11 him from having the earliest opportunity to guard himself against the Data Breach's  
12 harmful effects.

13       **Branislav Sasic**

14       72. Plaintiff Branislav Sasic is a resident and citizen of Frisco, Texas. Mr.  
15 Sasic does not recall having applied for a loan or refinance through loanDepot, or  
16 otherwise recall having been a loanDepot customer, and does not know or recall how  
17 loanDepot obtained his Private Information. Had Mr. Sasic known that loanDepot  
18 possessed his Private Information, he would have expected loanDepot to use  
19 reasonable measures to protect it in accordance with loanDepot's internal policies, as  
20 well as state and federal law.

21       73. Mr. Sasic is careful about sharing his sensitive Private Information. Mr.  
22 Sasic first learned of the Data Breach after receiving a data breach notification letter  
23 in or around March 2024, from loanDepot, notifying him of the Data Breach and that  
24 his Private Information had been improperly accessed and acquired by unauthorized  
25 third parties. Although he has never been a loanDepot customer and did not know  
26 loanDepot possessed his Private Information, Mr. Sasic still took the notice seriously,  
27 and made reasonable efforts to mitigate the impact thereof. In the time following the  
28 Data Breach, Mr. Sasic has experienced an issue when renewing his auto and

1 homeowner insurance policy, resulting in an almost \$2,000 increase in premium due  
2 to a "no hit" on his credit. Mr. Sasic has and is additionally experiencing fear, stress,  
3 and frustration because loanDepot disclosed his Private Information, which he does  
4 not recall providing to loanDepot, to unauthorized parties who may now use that  
5 information for unknown purposes. Mr. Sasic suffered actual injuries in the form of  
6 damages to and diminution in the value of his Private Information—a form of  
7 intangible property entrusted to loanDepot, which was compromised in and as a  
8 proximate result of the Data Breach. Mr. Sasic has suffered and will continue to suffer  
9 for the remainder of his life imminent and impending injury arising from the  
10 substantially increased risk of fraud, identity theft, and misuse proximately resulting  
11 from his Private Information being obtained by unauthorized third parties and/or  
12 cybercriminals.

13         74. Mr. Sasic has a continuing interest in ensuring that his Private  
14 Information, which remains within loanDepot's possession and control, is protected  
15 and safeguarded against future data breaches and cybersecurity risks. The delayed  
16 notification provided by loanDepot further impacted Mr. Sasic because it prevented  
17 him from having the earliest opportunity to guard himself against the Data Breach's  
18 harmful effects.

19         **Jessica Schuler**

20         75. Plaintiff Jessica Schuler is a resident and citizen of Gainesville, Florida.  
21 Ms. Schuler does not recall having applied for a loan or refinance through loanDepot,  
22 or otherwise recall having been a loanDepot customer. Had Ms. Schuler known that  
23 loanDepot possessed her Private Information, she would have expected loanDepot to  
24 use reasonable measures to protect it in accordance with loanDepot's internal policies,  
25 as well as state and federal law.

26         76. Ms. Schuler is careful about sharing her sensitive Private Information.  
27 Ms. Schuler first learned of the Data Breach after receiving a data breach notification  
28 letter in or around March 2024, from loanDepot, notifying her of the Data Breach and

1 that her Private Information, including her social security number, had been  
2 improperly accessed and acquired by unauthorized third parties. Although she has  
3 never been a loanDepot customer and did not know loanDepot possessed her Private  
4 Information, Ms. Schuler still took the notice seriously, and made reasonable efforts  
5 to mitigate the impact thereof, including, but not limited to, purchasing an identity  
6 theft prevention service and freezing her credit. In the time following the Data Breach,  
7 Ms. Schuler has experienced an increase in spam phone calls, emails, and spam text  
8 messages. Ms. Schuler has and is additionally experiencing fear, stress, and frustration  
9 because loanDepot disclosed her Private Information, which she does not recall  
10 providing to loanDepot, to unauthorized parties who may now use that information  
11 for unknown purposes. Ms. Schuler suffered actual injuries in the form of damages to  
12 and diminution in the value of her Private Information—a form of intangible property  
13 entrusted to loanDepot, which was compromised in and as a proximate result of the  
14 Data Breach. Ms. Schuler has suffered and will continue to suffer for the remainder  
15 of her life imminent and impending injury arising from the substantially increased  
16 risk of fraud, identity theft, and misuse proximately resulting from her Private  
17 Information being obtained by unauthorized third parties and/or cybercriminals.

18         77. Ms. Schuler has a continuing interest in ensuring that her Private  
19 Information, which remains within loanDepot's possession and control, is protected  
20 and safeguarded against future data breaches and cybersecurity risks. The delayed  
21 notification provided by loanDepot further impacted Ms. Schuler because it prevented  
22 her from having the earliest opportunity to guard herself against the Data Breach's  
23 harmful effects.

24         **Kyle Nunnelly**

25         78. Plaintiff Kyle Nunnelly is a resident and citizen of Westland, Michigan.  
26 Mr. Nunnelly does not recall having applied for a loan or refinance through  
27 loanDepot, or otherwise recall having been a loanDepot customer, and does not know  
28 or recall how loanDepot obtained his Private Information. Had Mr. Nunnelly known

1 that loanDepot possessed his Private Information, he would have expected loanDepot  
2 to use reasonable measures to protect it in accordance with loanDepot's internal  
3 policies, as well as state and federal law.

4 79. Mr. Nunnelly is careful about sharing his sensitive Private Information.  
5 Mr. Nunnelly first learned of the Data Breach after receiving a data breach notification  
6 letter in or around March 2024, from loanDepot, notifying him of the Data Breach  
7 and that his Private Information, including his social security number, had been  
8 improperly accessed and acquired by unauthorized third parties. Although he has  
9 never been a loanDepot customer and did not know loanDepot possessed his Private  
10 Information, Mr. Nunnelly still took the notice seriously, and made reasonable efforts  
11 to mitigate the impact thereof, including, but not limited to, purchasing an identity  
12 theft prevention service and placing a freeze on his credit with all three credit bureaus.  
13 In the time following the Data Breach, Mr. Nunnelly has experienced an increase in  
14 spam calls. Mr. Nunnelly has and is additionally experiencing fear, stress, and  
15 frustration because loanDepot disclosed his Private Information, which he does not  
16 recall providing to loanDepot, to unauthorized parties who may now use that  
17 information for unknown purposes. Mr. Nunnelly suffered actual injuries in the form  
18 of damages to and diminution in the value of his Private Information—a form of  
19 intangible property entrusted to loanDepot, which was compromised in and as a  
20 proximate result of the Data Breach. Mr. Nunnelly has suffered and will continue to  
21 suffer for the remainder of his life imminent and impending injury arising from the  
22 substantially increased risk of fraud, identity theft, and misuse proximately resulting  
23 from his Private Information being obtained by unauthorized third parties and/or  
24 cybercriminals.

25 80. Mr. Nunnelly has a continuing interest in ensuring that his Private  
26 Information, which remains within loanDepot's possession and control, is protected  
27 and safeguarded against future data breaches and cybersecurity risks. The delayed  
28 notification provided by loanDepot further impacted Mr. Nunnelly because it

1 prevented him from having the earliest opportunity to guard himself against the Data  
2 Breach's harmful effects.

3 **Matthew McFall**

4 81. Plaintiff Matthew McFall is a resident and citizen of Downers Grove,  
5 Illinois. Mr. McFall does not recall having applied for a loan or refinance through  
6 loanDepot, or otherwise recall having been a loanDepot customer, and does not know  
7 or recall how loanDepot obtained his Private Information. Had Mr. McFall known  
8 that loanDepot possessed his Private Information, he would have expected loanDepot  
9 to use reasonable measures to protect it in accordance with loanDepot's internal  
10 policies, as well as state and federal law.

11 82. Mr. McFall is careful about sharing his sensitive Private Information.  
12 Mr. McFall first learned of the Data Breach after receiving a data breach notification  
13 letter dated February 23, 2024, from loanDepot, notifying him of the Data Breach and  
14 that his Private Information, including his social security number, had been  
15 improperly accessed and acquired by unauthorized third parties. Although he has  
16 never been a loanDepot customer and did not know loanDepot possessed his Private  
17 Information, Mr. McFall still took the notice seriously and made reasonable efforts to  
18 mitigate the impact thereof. In the time following the Data Breach, Mr. McFall has  
19 experienced an increase in spam calls and text messages and an unauthorized attempt  
20 to change the name on his mortgage. Mr. McFall has and is additionally experiencing  
21 fear, stress, and frustration because loanDepot disclosed his Private Information,  
22 which he does not recall providing to loanDepot, to unauthorized parties who may  
23 now use that information for unknown purposes. Mr. McFall suffered actual injuries  
24 in the form of damages to and diminution in the value of his Private Information—a  
25 form of intangible property entrusted to loanDepot, which was compromised in and  
26 as a proximate result of the Data Breach. Mr. McFall has suffered and will continue  
27 to suffer for the remainder of his life imminent and impending injury arising from the  
28 substantially increased risk of fraud, identity theft, and misuse proximately resulting



1 from his Private Information being obtained by unauthorized third parties and/or  
2 cybercriminals.

3 83. Mr. McFall has a continuing interest in ensuring that his Private  
4 Information, which remains within loanDepot's possession and control, is protected  
5 and safeguarded against future data breaches and cybersecurity risks. The delayed  
6 notification provided by loanDepot further impacted Mr. McFall because it prevented  
7 him from having the earliest opportunity to guard himself against the Data Breach's  
8 harmful effects.

9 **B. Defendant**

10 84. loanDepot is an Irvine, California-based nonbank company that sells  
11 mortgage and non-mortgage lending products. loanDepot is a corporation formed in  
12 Delaware and registered in California, with a principal place of business located at  
13 6561 Irvine Center Drive, Irvine, California.

14 **III. JURISDICTION AND VENUE**

15 85. This Court has subject matter jurisdiction over this action pursuant to 28  
16 U.S.C. § 1332(d)(2), as amended by the Class Action Fairness Act of 2005, because  
17 (1) the amount in controversy in this class action exceeds five million dollars  
18 (\$5,000,000), excluding interest and costs; (2) there are more than 100 Class  
19 Members; (3) at least one Class Member is diverse from Defendant; and (4) the  
20 Defendant is not a government entity.

21 86. This Court has personal jurisdiction over Defendant because Defendant  
22 and/or its parents or affiliates are headquartered in this District and Defendant  
23 conducts substantial business in California and in this District through its  
24 headquarters, offices, parents, and affiliates.

25 87. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because  
26 Defendant's principal place of business is in this District and a substantial part of the  
27 events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District.

28 //

1 **IV. FACTS**

2 **A. loanDepot Collects, Stores, and Maintains Substantial Amounts of**  
 3 **Private Information, Which it Ensured it Would Safeguard**

4 88. loanDepot is a California-based retail mortgage lender and nonbank  
 5 holding company. It is the country's fifth-largest retail mortgage lender and the  
 6 second largest nonbank retail originator. Since its founding in 2010, Defendant has  
 7 provided more than \$275 billion in lending. loanDepot currently employs more than  
 8 6,000 individuals and services more than 27,000 customers each month.<sup>15</sup>

9 89. To utilize loanDepot's services, customers are required to provide  
 10 loanDepot with a large quantity of highly sensitive and private information;  
 11 loanDepot collects and maintains its customer's Private Information in its computer  
 12 systems, servers, and networks. On its privacy policy webpage, loanDepot admits to  
 13 collecting the following confidential and sensitive consumer Private Information<sup>16</sup>:

**Information We Collect**

***Consumer and Customers***

We collect information about you to help us serve your financial, real estate, insurance, credit, and homeownership-related needs; to provide you with quality products and services; and to fulfill legal and regulatory requirements. We consider non-public information about you in our possession to be personally identifiable information, even if you cease to be a customer. The personally identifiable information we collect about you may include:

- Identifying information, such as your name, age, address, phone number and social security number
- Employment information
- Contact information (such as first and last name, mailing or property address, phone number, email address)
- Account access information, such as username and password
- Demographic information (such as date of birth, gender, marital status, ethnicity, race)
- Social security, driver's license, passport, and other government identification numbers
- Loan account information (such as loan number)
- Bank account and credit/debit card numbers
- Other personal information needed from you to provide real estate-related, loan-related, insurance-related, credit-related, and homeownership-related services to you
- Information for fraud detection and prevention
- Financial information such as your income, assets and liabilities, as well as information about your savings, investments, insurance and business.

15 *See, supra*, n. 2.

16 *Supra*, n. 12.

1           90. Defendant is and was aware of the sensitive nature of the Private  
2 Information it collects, and the importance of safeguarding it.

3           91. In fact, Defendant acknowledged the significant risks of collecting and  
4 maintaining Private Information. In Defendant's Privacy Policy, it advanced a litany  
5 of assurances and promises to its customers that it will maintain the security and  
6 privacy of their personal information<sup>17</sup>:

**Safeguarding Personally Identifiable Information**

- We have adopted policies and procedures designed to protect your personally identifiable information from unauthorized use or disclosure.
- We have implemented physical, electronic, and procedural safeguards to maintain confidentiality and integrity of the personal information in our possession and to guard against unauthorized access. These include among other things, procedures for controlling access to your files, building security programs and information technology security measures such as the use of passwords, firewalls, virus prevention and use detection software.
- We continue to assess new technology as it becomes available and to upgrade our physical and electronic security systems as appropriate.
- Our policy is to permit employees to access your personal information only if they have a business purpose for using such information, such as administering, providing or developing our products or services.
- Our policy, which governs the conduct of all of our employees, requires all employees to safeguard personally identifiable information about the consumers and customers we serve or have served in the past.

**loanDepot Security Policy**

loanDepot takes steps to safeguard your personal and sensitive information through industry standard physical, electronic, and operational policies and practices. All data that is considered highly confidential data can only be read or written through defined service access points, the use of which is password-protected. The physical security of the data is achieved through a combination of network firewalls and servers with tested operating systems, all housed in a secure facility. Access to the system, both physical and electronic, is controlled and sanctioned by a high-ranking manager.

19           92. Defendant made numerous promises to Plaintiffs and Class Members  
20 that they would maintain the security and privacy of their Private Information. For  
21 instance, in its Privacy Policy, Defendant assures consumers that while it shares  
22 customers' Private Information with third parties "as required or permitted by law,"  
23 Defendant's "policy is to require third-party service providers to enter into  
24 confidentiality agreements with [loanDepot], prohibiting them from using any  
25 personally identifiable information they obtain for any other purpose other than those  
26

27  
28 <sup>17</sup> *Id.*

1 for which they were retained or as required by law.”<sup>18</sup>

2 93. Defendant provided each of its applicants and customers with a copy of  
3 its Privacy Policy and other policies and required each customer to sign an  
4 acknowledgment of the terms thereof. Based on further information and belief,  
5 loanDepot was otherwise bound by the representations made in these agreements,  
6 regardless of whether Plaintiffs and/or Class Members executed an acknowledgment,  
7 by its acceptance of Plaintiffs’ and Class Members’ Private Information.

8 94. Through these policies, among others, loanDepot made promises to  
9 Plaintiffs and Class Members that it would protect their Private Information by  
10 maintaining adequate data security, acknowledged that it was a predictable target of  
11 unauthorized parties for a data breach, such as the Data Breach, and led Plaintiffs and  
12 Class Members to believe loanDepot could be trusted with their Private Information.  
13 By failing to protect Plaintiffs’ and Class members’ Private Information, by allowing  
14 the Data Breach to occur, and otherwise disclosing Plaintiffs’ and Class Members’  
15 Private Information, Defendant broke these privacy promises.

16 95. Plaintiffs and Class Members took reasonable steps to maintain the  
17 confidentiality of their Private Information and relied on Defendant to keep their  
18 Private Information confidential and securely maintained.

19 96. By obtaining, collecting, using, and deriving a benefit from Plaintiffs’  
20 and Class Members’ Private Information, Defendant assumed legal, equitable, and  
21 affirmative duties to safeguard their Private Information.

22 97. Plaintiffs and Class Members relied on Defendant to implement and  
23 follow adequate data security policies and protocols, to keep their Private Information  
24 confidential and securely maintained, to use such Private Information solely for  
25 business purposes, and to prevent the unauthorized disclosure of Private Information.

26 //

27  
28 <sup>18</sup> *Id.*

1        98. Despite these extensive proclaimed proactive policies and approaches to  
 2 maintain data security and privacy for its customers, loanDepot failed to adequately  
 3 safeguard its systems and networks from a foreseeable and preventable cyberattack.  
 4 This conduct proximately caused the Data Breach and significant, irreparable harm to  
 5 Plaintiffs and Class Members.

6        **B. The Data Breach: loanDepot Failed to Safeguard Valuable**  
 7        **Consumer Private Information**

8        99. On or around January 8, 2024, loanDepot posted the following online:  
 9 loanDepot is experiencing a cyber incident.

10        We have taken certain systems offline and are working diligently to  
 11 restore normal business operations as quickly as possible. We are  
 12 working quickly to understand the extent of the incident and taking steps  
 13 to minimize its impact. The Company has retained leading forensics  
 14 experts to aid in our investigation and is working with law enforcement.  
 15 We sincerely apologize for any impacts to our customers and we are  
 16 focused on resolving these matters as soon as possible.<sup>19</sup>

17        100. Following the breach, Defendant intermittently posted updates to its  
 18 website alerting customers when its various subsidiaries' payment portals were  
 19 reactivated. On or about January 22, 2024, Defendant posted the following statement  
 20 in response to the Data Breach:

21        The Company has been working diligently with outside forensics and  
 22 security experts to investigate the incident and restore normal operations  
 23 as quickly as possible. The Company has made significant progress in  
 24 restoring our loan origination and loan servicing systems, including our  
 25 MyloanDepot and Servicing customer portals.

26        Although its investigation is ongoing, the Company has determined that  
 27 an unauthorized third party gained access to sensitive personal  
 28 information of approximately 16.6 million individuals in its systems. The  
 Company will notify these individuals and offer credit monitoring and  
 identity protection services at no cost to them.

<sup>19</sup> *loanDepot is experiencing a cyber incident*, loanDepot,  
<https://loandepot.cyberincidentupdate.com/> (last visited May 30, 2024).

1 “Unfortunately, we live in a world where these types of attacks are  
 2 increasingly frequent and sophisticated, and our industry has not been  
 3 spared. We sincerely regret any impact on our customers,” said  
 4 loanDepot CEO Frank Martell. “The entire loanDepot team has worked  
 5 tirelessly throughout this incident to support our customers, our partners  
 6 and each other. I am pleased by our progress in quickly bringing our  
 7 systems back online and restoring normal business operations.”

8 “Our customers are at the center of everything we do,” said Jeff Walsh,  
 9 President of loanDepot Mortgage. “I’m really proud of our team, and  
 10 we’re glad to be back to doing what we do best: enabling our customers  
 11 across the country to achieve their financial goals and dreams of  
 12 homeownership.”

13 The Company is committed to keeping its customers, partners, and  
 14 employees informed and will provide any additional operational updates  
 15 on our microsite at [loandepot.cyberincidentupdate.com](https://loandepot.cyberincidentupdate.com).<sup>20</sup>

16 101. Although loanDepot claimed to be working to restore “normal”  
 17 operations, there was no acknowledgment that the insufficiency of “normal”  
 18 operations led to the Data Breach in the first place. loanDepot did not express any  
 19 desire to change, update, or otherwise improve security and other protocols which  
 20 clearly failed here, let alone provide any clear explanation of what new security  
 21 protocols and safeguards it will put in place.

22 //

23 //

24 //

25 //

26 //

27 //

28 //

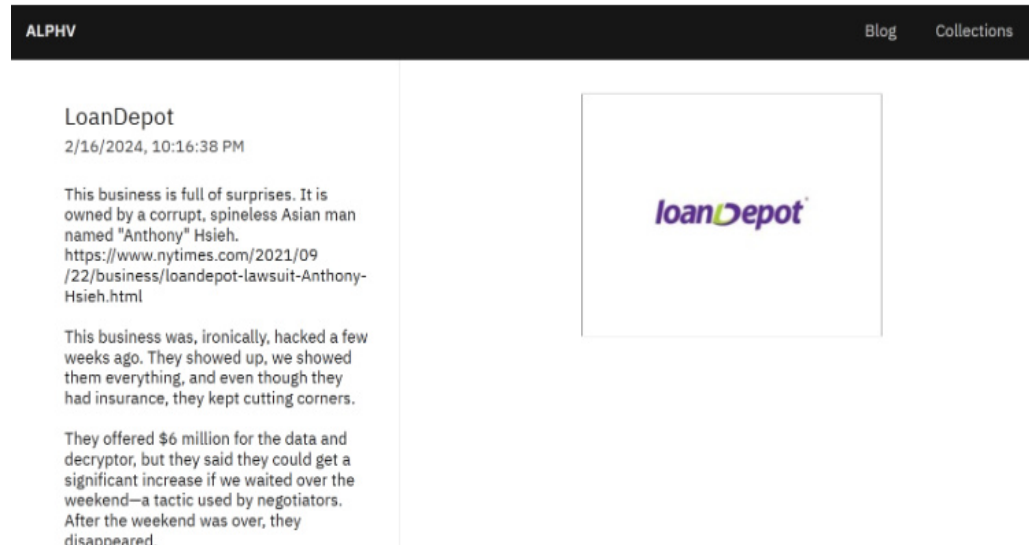
29 //

30 //

---

<sup>20</sup> *Supra*, n. 4.

102. On February 16, 2024, the ALPHV/BlackCat ransomware gang publicly identified themselves and claimed credit for the Data Breach. ALPHV/BlackCat named the home lender on its leak blog on February 16th, accompanied by a lengthy post singling out the company for “cutting corners” and failing to pay a ransom<sup>21</sup>:



103. In ALPHV’s post, it also called out the online mortgage firm for not disclosing “the full amount of data stolen.” The group stated: “We downloaded multiple databases from credit bureaus that included personal information about American citizens, even those who had never applied for any of their products From [sic] their accesses.” Furthermore, ALPHV claims loanDepot “withheld information about 4 TB of additional data that included comprehensive client data.”<sup>22</sup>

104. The threat actors also provided considerable information about loanDepot’s failure to pay the ransom. The gang blamed the so-called failed ransom negotiations on the company’s legal team, insurance underwriters, and being “unable to make up their minds.” “They offered \$6 million for the data and decryptor... we waited over the weekend—a tactic used by negotiators. After the weekend was over, they disappeared,” ALPHV wrote.<sup>23</sup>

<sup>21</sup> See, *supra*, n. 10.

<sup>22</sup> *Id.*

<sup>23</sup> *Id.*



1           105. Additionally, the gang implied it had sources at the company feeding  
 2 them inside information. “The CIO [Chief Information Officer] was 10 steps behind  
 3 us and was feeding the Executive team false information on purpose. Our insiders at  
 4 this company informed us that they were being pressured to leave [the negotiations]  
 5 by their outside counsel,” the post said. “As their networks were being taken over,  
 6 they took weeks to make a decision... and finally turned to leave” ALPHV added.<sup>24</sup>

7           106. Due to the failed negotiations over a ransom, the threat actors monetized  
 8 the stolen data by selling it, writing “Your information is in the final process of being  
 9 sold. That’s all . . . .”<sup>25</sup>

10           107. ALPHV/BlackCat is a well-known threat actor that first appeared in  
 11 2021. Known for its triple-extortion tactics, the gang was responsible for the  
 12 September 2023 ransomware attacks on the Las Vegas casino giants MGM Resorts  
 13 and Caesars International. ALPHV/BlackCat is a known threat that Defendant chose  
 14 to ignore.

15           108. True to their word, ALPHV/BlackCat had posted loanDepot’s data on  
 16 their website:

17 //

18 //

19 //

20 //

21 //

22 //

23 //

24 //

25 //

26 //

27 \_\_\_\_\_  
 28 <sup>24</sup> *Id.*

<sup>25</sup> *Id.*

## alphv

parsing : enabled

aka blackcat - fileservers ihogunvdybry6kileinjc3ic6du6arh3arouxr6ddswxa2wbyd.onion

- <https://therecord.media/alphv-blackcat-is-the-first-professional-ransomware-gang-to-use-rust/>
- <https://www.bleepingcomputer.com/news/security/alphv-blackcat-this-years-most-sophisticated-ransomware/>
- <https://securityaffairs.co/wordpress/126072/cyber-crime/inetum-hit-by-blackcat-ransomware.html>
- <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/noberus-blackcat-alphv-rust-ransomware>

title	available	version	last visit	fqdn
404 Not Found	True	3	12:14 30/05/2024	alphvmm27o3eb03r2mlejrpdm2le3rykajqcsj7j7ejksbpa3ed.onion
none	False	3	00:00 01/05/2021	2cuageerj8ba2rhdiviezodpu1lo4qr2ajf4qn6f7std2evleqlzjid.onion
404 Not Found	True	3	12:14 30/05/2024	vqifx1lrequdvulh3zac5gocbeaw167uvs2pttewendorbnhdddyd.onion
Error response	False	3	15:13 09/03/2024	alphvuzxyvdy1umd2ng046x2qpw6zf1oerghvxeu6k1lberbttyd.onion

post	date
ipmeltanira	03/03/2024
Exig Usa	03/03/2024
Petrus Resources Ltd.	02/03/2024
SBH & Co [You have 48 hours. Check your e-mail]	02/03/2024
Kumagai Gumi Group	01/03/2024
Allen Berger & Associates	29/02/2024
Change Healthcare - Optum - UnitedHealth	28/02/2024
verbraucherzentrale hessen	27/02/2024
Electro Martelx	27/02/2024
Angeles Medical Centers	26/02/2024
SVC Partners	26/02/2024
Northern Industries [FULL DATA]	24/02/2024
Family Health center	23/02/2024
ANDFLA SRL	23/02/2024
Hardeman County Community Health Center	22/02/2024
Northern Industries [We're giving you one last chance to save your business]	22/02/2024
KHDS [You have 3 days]	21/02/2024
Austen Consultants	21/02/2024
VSP Dental	18/02/2024
Prudential Financial	16/02/2024
LoanDepot	16/02/2024
Rush Energy Services Inc [Time's up]	15/02/2024
ASA Electronics [2.7 TB]	15/02/2024
The Source	13/02/2024

109. Subsequently on or about February 23, 2024, almost six weeks after the January 8, 2024 announcement and SEC filing, Defendant finally began to provide notice of the Data Breach to its customers, employees, and states' attorneys general.<sup>26</sup> The size of this already massive breach grew to 16,924,071. Defendant also offered 24 months of single-bureau credit monitoring through Experian.

110. Defendant's disclosures did not mention anything about the threat actor, or the fact that highly confidential Private Information including SSNs was exfiltrated by a well-known ransomware gang that publicly announced it was in the final stages of selling the data. Instead, the Notice Letters speak in vague terms about customer data that "may have been accessed."<sup>27</sup>

<sup>26</sup> See, *supra*, n. 1.

<sup>27</sup> *Id.*

111. The unreasonable delay of action and prolonged exposure of almost 17 million customers' Private Information has unreasonably exacerbated the harms caused by the Data Breach by denying affected individuals the opportunity to proactively protect their Private Information from misuse as a result of the Data Breach.

112. Defendant acknowledged in a subsequent Form 8-K filing that the attackers not only acquired customer data, but that they also "access[ed] certain Company systems," encrypted data, and forced Defendant to shut down customer portals and other tools in response to the attack.<sup>28</sup>

113. Defendant could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting its equipment and computer files containing Private Information. Defendant could also have employed multi-factor authentication to ensure that compromised passwords could not be used by unauthorized individuals.

114. A ransomware attack is a type of cyberattack that is frequently used to target companies due to the sensitive data they maintain.<sup>29</sup> In a ransomware attack, the attackers use software to encrypt data on a compromised network, rendering it unusable and demanding payment to restore control over the network.<sup>30</sup>

115. Companies should treat ransomware attacks as any other data breach incident because ransomware attacks don't just hold networks hostage, "ransomware

---

<sup>28</sup> Sergiu Gatlan, *US mortgage lender loanDepot confirms ransomware attack*, BleepingComputer (Jan. 8, 2024, 12:39 p.m.), <https://www.bleepingcomputer.com/news/security/us-mortgage-lender-loandepot-confirms-ransomware-attack/>.

<sup>29</sup> Danny Palmer, *Ransomware warning: Now attacks are stealing data as well as encrypting it*, ZDNET (July 14, 2020, 8:28 a.m. PT), <https://www.zdnet.com/article/ransomware-warning-now-attacks-are-stealing-data-as-well-as-encrypting-it/>.

<sup>30</sup> *Ransomware FAQs*, Stop Ransomware, <https://www.cisa.gov/stopransomware/ransomware-faqs> (last visited May 30, 2024).

1 groups sell stolen data in cybercriminal forums and dark web marketplaces for  
 2 additional revenue.”<sup>31</sup> As cybersecurity expert Emsisoft warns, “[a]n absence of  
 3 evidence of exfiltration should not be construed to be evidence of its absence [...] the  
 4 initial assumption should be that data may have been exfiltrated.”<sup>32</sup>

5 116. An increasingly prevalent form of ransomware attack is the  
 6 “encryption+exfiltration” attack, in which the attacker encrypts a network and  
 7 exfiltrates the data contained within.<sup>33</sup> In 2020, over 50% of ransomware attackers  
 8 exfiltrated data from a network before encrypting it.<sup>34</sup> Once the data is exfiltrated  
 9 from a network, its confidential nature is destroyed and it should be “assume[d] it will  
 10 be traded to other threat actors, sold, or held for a second/future extortion attempt.”<sup>35</sup>  
 11 And even where companies pay for the return of data attackers often leak or sell the  
 12 data regardless because there is no way to verify copies of the data are destroyed.<sup>36</sup>

13 117. Based upon the public statements of the threat actors, their reputation for  
 14 “triple extortion” ransomware attacks, and Defendant’s own Form 8-K statement  
 15 acknowledging exfiltration, this ransomware attack was designed to not just encrypt  
 16 Defendant’s systems, but also to steal and monetize massive amounts of Private  
 17 Information.

18 118. As explained by the Federal Bureau of Investigation, “[p]revention is the  
 19 most effective defense against ransomware and it is critical to take precautions for  
 20

21 <sup>31</sup> *Ransomware: The Data Exfiltration and Double Extortion Trends*, Center for  
 22 Internet Security, <https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trends> (last visited May 30, 2024).

23 <sup>32</sup> *The chance of data being stolen in a ransomware attack is greater than one in*  
 24 *ten*, Emsisoft Malware Lab (July 13, 2020), <https://blog.emsisoft.com/en/36569/the-chance-of-data-being-stolen-in-a-ransomware-attack-is-greater-than-one-in-ten/>.

25 <sup>33</sup> *Id.*

26 <sup>34</sup> *Ransomware Demands continue to rise as Data Exfiltration becomes common,*  
 27 *and Maze subdues*, Coveware (November 4, 2020), <https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report>.

28 <sup>35</sup> *Id.*

<sup>36</sup> *Id.*

1 protection.”<sup>37</sup>

2 119. To prevent and detect cyber-attacks and/or ransomware attacks  
3 Defendant could and should have implemented, as recommended by the United States  
4 government, the following measures:

- 5 • Implement an awareness and training program. Because end  
6 users are targets, employees and individuals should be aware of  
7 the threat of ransomware and how it is delivered;
- 8 • Enable strong spam filters to prevent phishing emails from  
9 reaching the end users and authenticate inbound email using  
10 technologies like Sender Policy Framework (SPF), Domain  
11 Message Authentication Reporting and Conformance (DMARC),  
12 and DomainKeys Identified Mail (DKIM) to prevent email  
13 spoofing;
- 14 • Scan all incoming and outgoing emails to detect threats and filter  
15 executable files from reaching end users;
- 16 • Configure firewalls to block access to known malicious IP  
17 addresses;
- 18 • Patch operating systems, software, and firmware on devices.  
19 Consider using a centralized patch management system;
- 20 • Set anti-virus and anti-malware programs to conduct regular  
21 scans automatically;
- 22 • Manage the use of privileged accounts based on the principle of  
23 least privilege: no users should be assigned administrative access  
24 unless absolutely needed; and those with a need for administrator  
25 accounts should only use them when necessary;
- 26 • Configure access controls—including file, directory, and  
27 network share permissions—with least privilege in mind. If a  
28 user only needs to read specific files, the user should not have  
written access to those files, directories, or shares;
- Disable macro scripts from office files transmitted via email.  
Consider using Office Viewer software to open Microsoft Office  
files transmitted via email instead of full office suite

---

<sup>37</sup> *How to Protect Your Networks from Ransomware*, FBI.gov,  
<https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view> (last visited May 30, 2024).

1 applications;

- 2 • Implement Software Restriction Policies (SRP) or other controls
- 3 to prevent programs from executing from common ransomware
- 4 locations, such as temporary folders supporting popular Internet
- 5 browsers or compression/decompression programs, including the
- 6 AppData/LocalAppData folder;
- 7 • Consider disabling Remote Desktop protocol (RDP) if it is not
- 8 being used;
- 9 • Use application whitelisting, which only allows systems to
- 10 execute programs known and permitted by security policy;
- 11 • Execute operating system environments or specific programs in a
- 12 virtualized environment; and
- 13 • Categorize data based on organizational value and implement
- 14 physical and logical separation of networks and data for different
- 15 organizational units.<sup>38</sup>

16 120. To prevent and detect cyber-attacks or ransomware attacks, Defendant  
 17 could and should have implemented, as recommended by the Microsoft Threat  
 18 Protection Intelligence Team, several measures, including applying the latest security  
 19 updates, thoroughly investigating and mediating alerts, collaborating with IT  
 20 professionals about security operations, using multifactor authentication and network-  
 21 level authentication, and strengthening Defendant's infrastructure.<sup>39</sup>

22 121. Given that Defendant was storing the sensitive Private Information of its  
 23 current and former customers and applicants, Defendant could and should have  
 24 implemented the above measures to prevent and detect cyberattacks.

25 122. In response to the Data Breach, loanDepot admits it worked with external  
 26 "security experts" to determine the nature and scope of the incident and purports to  
 27 have taken steps to secure the systems. loanDepot admits additional security was

---

28 <sup>38</sup> *Id.* at 3-4.

<sup>39</sup> Microsoft Threat Intelligence, *Human-operated Ransomware Attacks: A Preventable Disaster*, Microsoft (Mar 5, 2020), <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/>.

1 required, but there is no indication whether these steps are adequate to protect  
2 Plaintiffs' and Class Members' Private Information going forward.

3 **C. loanDepot Had Ample Notice of Its Computer Systems'**  
4 **Vulnerabilities and That It Was a Likely Cyberattack Target**

5 123. Given the valuable Private Information that Plaintiffs and Class  
6 Members entrusted loanDepot with, its prior data breach and the escalating frequency  
7 of cyberattacks in the finance industry, loanDepot knew, or should have known, at all  
8 relevant times, that it was vulnerable to and at a heightened risk of cyberattacks.

9 124. loanDepot was on notice that it was actively targeted by hackers. In  
10 August 2022, loanDepot was subject to a separate cyberattack. The attack exposed  
11 tens of thousands of documents that included customers' Private Information and  
12 impacted well over a thousand individuals.<sup>40</sup>

13 125. Nine months after the August 2022 breach, on May 8, 2023, loanDepot  
14 notified customers that their information had been stolen in a cyberattack.<sup>41</sup> In light  
15 of the stringent laws mandating companies to immediately report data breaches,  
16 loanDepot's failure to report the August 2022 data breach for nine months suggests  
17 that loanDepot's systems were so deficient and inadequate that loanDepot did not  
18 know, for an unreasonably protracted period, that it had been hacked.

19 126. loanDepot knew or should have known the high probability of additional  
20 sophisticated attacks, and that additional significant security measures were necessary  
21 to prevent further breaches. Nonetheless, despite the significant August 2022 data  
22 breach, loanDepot failed to invest adequate resources required to improve its data  
23 security, thus continuing to expose its customers to a foreseeable and significant risk  
24 of another data breach.

25  
26 <sup>40</sup> *Data Security Event*, loanDepot (April 24, 2023),  
27 <https://www.doj.nh.gov/consumer/security-breaches/documents/loandepot-20230424.pdf>.

28 <sup>41</sup> *Id.*



1           127. In addition to being on notice of its systems’ security vulnerabilities  
2 following its August 2022 data breach, loanDepot knew or should have known that it  
3 was at a heightened risk of a cyberattack due to the surge of cyberattacks and/or data  
4 breaches the mortgage industry was and has been experiencing.

5           128. In October 2023, in response to the increasing prevalence of cyberattacks  
6 in the mortgage and real estate industry, the United States Federal Trade Commission  
7 (“FTC”) finalized an amendment to the Safeguards Rule that requires mortgage  
8 originators, like loanDepot, to report certain data breaches and other security events  
9 affecting 500 or more customers to the FTC as soon as possible, but no later than 30  
10 days.

11           129. In the third quarter of the 2023 fiscal year alone, 733 organizations  
12 experienced data breaches, resulting in 66,658,764 individuals’ personal information  
13 being compromised.<sup>42</sup>

14           130. Due to high profile data breaches at other large companies and because  
15 these attacks have become ubiquitous, Defendant knew or should have known that it  
16 was a prime target due to the vast amount of Private Information that it collected and  
17 maintained in the regular course of its business.

18           131. The increase in such attacks, and attendant risk of future cyberattacks,  
19 was widely known to the public and to anyone in Defendant’s industry, including  
20 Defendant.

21           132. Defendant’s CEO Frank Martel publicly affirmed loanDepot’s  
22 knowledge of these risks when he stated: “we live in a world where these types of  
23 attacks are increasingly frequent and sophisticated, and our industry has not been  
24 spared.”<sup>43</sup>

25  
26 <sup>42</sup> *ITRC Q3 Data Breach Analysis*, Identity Theft Resource Center,  
27 <https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/> (last visited  
28 May 30, 2024).

<sup>43</sup> *See, supra*, n. 4.

1           133. Given loanDepot's firsthand knowledge of its vulnerabilities to  
2 cyberattacks derived from its prior separate data breach in 2022, coupled with the  
3 prevailing industry knowledge of the pervasive uptick of data breaches, loanDepot  
4 knew or should have known that it was at a heightened risk of another data breach.

5           134. In light of the known risks and in violation of its representations to Class  
6 Members and its legal obligations, loanDepot failed to act to implement reasonable,  
7 expected, and readily available data security procedures and practices to protect  
8 against disclosure of its customers' Private Information.

9           **D. loanDepot Failed to Comply with FTC Guidelines and**  
10           **Requirements**

11           135. The FTC has promulgated numerous guides for businesses that highlight  
12 the importance of implementing reasonable data security practices. According to the  
13 FTC, the need for data security should be factored into all business decision-making.

14           136. In 2016, the FTC updated its publication, *Protecting Personal*  
15 *Information: A Guide for Business*, which established cyber-security guidelines for  
16 businesses.<sup>44</sup> The guidelines note that businesses should protect the personal customer  
17 information that they keep; properly dispose of personal information that is no longer  
18 needed; encrypt information stored on computer networks; understand its network's  
19 vulnerabilities; and implement policies to correct any security problems.<sup>45</sup> The  
20 guidelines also recommend that businesses use an intrusion detection system to  
21 expose a breach as soon as it occurs; monitor all incoming traffic for activity  
22 indicating someone is attempting to hack the system; watch for large amounts of data  
23 being transmitted from the system; and have a response plan ready in the event of a  
24 breach.<sup>46</sup>

25 \_\_\_\_\_  
26 <sup>44</sup> *Protecting Personal Information: A Guide for Business*, Federal Trade  
27 Commission (October 2016), [https://www.ftc.gov/system/files/documents/plain-  
language/pdf-0136\\_proteting-personal-information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf).

28 <sup>45</sup> *Id.*

<sup>46</sup> *Id.*

1           137. The FTC further recommends that companies not maintain Private  
 2 Information longer than is needed for authorization of a transaction; limit access to  
 3 sensitive data; require complex passwords to be used on networks; use industry-tested  
 4 methods for security; monitor for suspicious activity on the network; and verify that  
 5 third-party service providers have implemented reasonable security measures.

6           138. Pursuant to Section 5 of the Federal Trade Commission Act (the “FTC  
 7 Act”), 15 U.S.C. § 45, the FTC has brought enforcement actions against businesses  
 8 for failing to adequately and reasonably protect customer data. The FTC has treated  
 9 the failure to employ reasonable and appropriate measures to protect against  
 10 unauthorized access to confidential consumer data as an unfair business practice.

11           139. Orders resulting from these actions, including actions against mortgage  
 12 lenders, further clarify the measures businesses must take to meet their data security  
 13 obligations.

14           140. Defendant owed a duty to safeguard Plaintiffs’ and Class Members’  
 15 Private Information under FTC Act, 15 U.S.C. § 45, among other statutes further  
 16 discussed below, to ensure that all information it received, maintained, and stored was  
 17 secure. These statutes were enacted to protect Plaintiffs and Class Members from the  
 18 type of conduct in which Defendant engaged and the resulting harms Defendant  
 19 caused Plaintiffs and Class Members.

20           141. Defendant failed to properly implement basic data security measures to  
 21 protect against unauthorized access to customer Private Information, which  
 22 constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C.  
 23 § 45.

24           142. Had Defendant exercised reasonable care and properly maintained and  
 25 adequately protected its systems, servers, and networks in accordance with its duties,  
 26 the Data Breach would not have occurred or would have been detected and prevented.

27           **E. loanDepot Failed to Comply with Industry Standards**

28           143. As noted above, experts studying cyber security routinely identify

1 mortgage lenders and partners as being particularly vulnerable to cyberattacks  
2 because of the volume of the valuable Private Information which they collect and  
3 maintain.

4 144. Several best practices that, at a minimum, should be implemented by  
5 companies that maintain Private Information, like Defendant, include but are not  
6 limited to: educating and training all employees; strong passwords; changing  
7 passwords frequently; multi-layer security, including firewalls, anti-virus, and anti-  
8 malware software; encryption, making data unreadable without a key; multi-factor  
9 authentication; backup data; retaining Private Information for limited amounts of  
10 time, and limiting access to sensitive data.

11 145. Other best cybersecurity practices that are standard in the mortgage  
12 industry include installing appropriate malware detection software; monitoring and  
13 limiting the network ports; protecting web browsers and email management systems;  
14 setting up network systems such as firewalls, switches and routers; monitoring and  
15 protection of physical security systems; protection against any possible  
16 communication system; and training staff regarding critical points.

17 146. Defendant also failed to meet the minimum standards of the following  
18 frameworks: the NIST Cybersecurity Framework Version 1.1 (including without  
19 limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1,  
20 PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8,  
21 and RS.CO-2), and the Center for Internet Security's Critical Security Controls ("CIS  
22 CSC"), which are all established standards in reasonable cybersecurity readiness.

23 147. The foregoing frameworks are applicable industry standards in the  
24 mortgage industry. Defendant failed to comply with these accepted standards, thereby  
25 opening the door to the cyber incident and causing the Data Breach.

26 148. Defendant's failure to comply with industry standard data security  
27 practices was directly contrary to the representations made to its customers and  
28 consumers in its Privacy Policy and constitutes material misrepresentations.

1           **F.    loanDepot Breached Its Duties to Plaintiffs and Class Members**

2           149. As a sophisticated business entity handling confidential Private  
3 Information, loanDepot's data security obligations were particularly important given  
4 the substantial increase in cyberattacks and/or data breaches in industries holding  
5 significant amounts of Private Information preceding the date of the Data Breach.

6           150. Defendant had obligations created by contract, industry standards,  
7 common law, and its own promises and representations made to Plaintiffs and Class  
8 Members to keep their Private Information confidential and to protect them from  
9 unauthorized access and disclosure.

10          151. Defendant breached its obligations to Plaintiffs and Class Members  
11 and/or was otherwise negligent and reckless because it failed to properly maintain and  
12 safeguard its computer systems and website's application flow, and intentionally  
13 misrepresented to Plaintiffs and Class Members the actions that it would take to  
14 protect their confidential information. Defendant's breaches of obligations include,  
15 but are not limited to, the following acts and/or omissions:

- 16           a.     failing to maintain an adequate data security system to reduce the  
17                   risk of data breaches and cyber-attacks;
- 18           b.     failing to adequately protect Private Information;
- 19           c.     failing to properly monitor its own data security systems for  
20                   existing intrusions;
- 21           d.     failing to ensure that its vendors with access to their computer  
22                   systems and data employed reasonable security procedures;
- 23           e.     failing to ensure the confidentiality and integrity of electronic  
24                   Private Information it created, received, maintained, and/or  
25                   transmitted;
- 26           f.     failing to implement technical policies and procedures for  
27                   electronic information systems that maintain electronic Private  
28                   Information to allow access only to those persons or software

- 1 programs that have been granted access rights;
- 2 g. failing to implement policies and procedures to prevent, detect,
- 3 contain, and correct security violations;
- 4 h. failing to implement procedures to review records of information
- 5 system activity regularly, such as audit logs, access reports, and
- 6 security incident tracking reports;
- 7 i. failing to protect against reasonably anticipated threats or hazards
- 8 to the security or integrity of electronic Private Information;
- 9 j. failing to train all members of its workforces effectively on the
- 10 policies and procedures regarding Private Information;
- 11 k. failing to render the electronic Private Information it maintained
- 12 unusable, unreadable, or indecipherable to unauthorized
- 13 individuals;
- 14 l. failing to comply with FTC guidelines for cybersecurity, in
- 15 violation of Section 5 of the FTC Act;
- 16 m. failing to adhere to industry standards for cybersecurity as
- 17 discussed above; and
- 18 n. otherwise breaching its duties and obligations to protect Plaintiffs’
- 19 and Class Members’ Private Information.

20 152. Defendant negligently and unlawfully failed to safeguard Plaintiffs’ and

21 Class Members’ Private Information by allowing third parties to access Defendant’s

22 unsecured and internet accessible networks, and to acquire and exfiltrate the

23 unencrypted Private Information.

24 153. Additionally, the law imposes an affirmative duty on Defendant to timely

25 disclose the unauthorized measures to mitigate damages, protect against adverse

26 consequences, and thwart future misuse of Private Information. loanDepot further

27 breached its duties by failing to provide reasonably timely notice of the Data Breach

28 to Plaintiffs and Class Members. In doing so, Defendant actually and proximately

1 caused and exacerbated Plaintiffs and Class Members' harm from the Data Breach  
2 and the injuries-in-fact.

3 154. Accordingly, as outlined below and in addition to other injuries resulting  
4 from the Data Breach, Plaintiffs and Class Members now face a continuing and  
5 imminent risk of fraud and identity theft. Moreover, due to the immutable information  
6 (e.g., SSNs) compromised in the Data Breach, Plaintiffs and Class Members will  
7 remain under this threat for the remainder of their lives.

8 **G. Plaintiffs' and Class Members' Private Information is Highly**  
9 **Valuable**

10 155. Private Information is an extremely valuable property right.<sup>47</sup> The value  
11 of sensitive personal information as a commodity is measurable.<sup>48</sup> Firms are now able  
12 to attain significant market valuations by employing business modes predicated on  
13 successful use of personal data within the existing legal and regulatory frameworks.<sup>49</sup>

14 156. Private Information is particularly valuable because criminals can use it  
15 to target victims with frauds and scams on an ongoing basis, rather than exploiting  
16 one account until it is canceled.

17 157. Private Information demands a much higher price on the black market.  
18 Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared  
19 to credit card information, personally identifiable information and Social Security  
20

21 <sup>47</sup> See, e.g., John T. Soma, et al, *Corporate Privacy Trend: The "Value" of*  
22 *Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*,  
15 RICH. J.L. & TECH. 11, at \*3-4 (2009) ("PII, which companies obtain at little  
23 cost, has quantifiable value that is rapidly reaching a level comparable to the value  
of traditional financial assets.") (citations omitted).

24 <sup>48</sup> Robert Lowes, *Stolen EHR Charts Sell for \$50 Each on Black Market*, Medscape  
25 (April 28, 2014), <https://www.medscape.com/viewarticle/824192?form=fpf>.

26 <sup>49</sup> OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies*  
27 *for Measuring Monetary Value*, OECD iLibrary (April 2, 2013), [https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-](https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en)  
28 [data\\_5k486qtxldmq-en](https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en) [https://www.networkworld.com/article/935334/anthem-](https://www.networkworld.com/article/935334/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html)  
[hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html](https://www.networkworld.com/article/935334/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html).



1 Numbers are worth more than 10x on the black market.”<sup>50</sup>

2 158. According to the United States Government Accountability Office  
3 (“USGAO”), which conducted a study regarding data breaches:

4 [L]aw enforcement officials told us that in some cases, stolen data may  
5 be held for up to a year or more before being used to commit identity  
6 theft. Further, once stolen data have been sold or posted on the Web,  
7 fraudulent use of that information may continue for years. As a result,  
8 studies that attempt to measure the harm resulting from data breaches  
9 cannot necessarily rule out all future harm.<sup>51</sup>

10 159. Private Information is such a valuable commodity to identity-thieves that  
11 once the information has been compromised, it is circulated and traded by criminals  
12 on the “cyber black-market” for years.

13 160. Because of the value of its collected and stored data, the financial  
14 industry has experienced disproportionately higher numbers of data theft events than  
15 other industries.

16 161. Based upon the public statements of the threat actors that they were in  
17 the final stages of selling the stolen data, there is a likelihood that entire batches of  
18 stolen information have already been dumped on the black market, or will be dumped  
19 on the black market, meaning Plaintiffs and Class Members are at an increased risk  
20 of fraud and identity theft for the foreseeable future and beyond.

21 162. An active and robust legitimate marketplace for Private Information also  
22 exists. In 2019, the data brokering industry was worth roughly \$200 billion.<sup>52</sup>

23 163. The data marketplace is so sophisticated that consumers can actually sell

24 <sup>50</sup> Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen*  
25 *Credit Card Numbers*, Network World (Feb. 6, 2015),  
26 <https://www.networkworld.com/article/935334/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html>.

27 <sup>51</sup> See, *supra*, n. 13.

28 <sup>52</sup> Ashiq JA, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/>.

1 their non-public information directly to a data broker who, in turn, aggregates the  
2 information and provides it to marketers or app developers.<sup>53,54</sup>

3 164. For instance, consumers who agree to provide their web browsing history  
4 to the Nielsen Corporation can receive up to \$50.00 a year.<sup>55</sup>

5 165. As a result of the Data Breach, Plaintiffs' and Class Members' Private  
6 Information, which has an inherent market value in both legitimate and dark markets,  
7 has been damaged and diminished by its compromise and unauthorized release.  
8 However, this transfer of value occurred without any consideration paid to Plaintiffs  
9 or Class Members for their property, resulting in an economic loss. Moreover, the  
10 Private Information is now readily available, and the rarity of the Data has been lost,  
11 thereby causing additional loss of value.

12 166. Defendant knew, or should have known, about these dangers and should  
13 have strengthened its data and email handling systems accordingly. Defendant was  
14 put on notice of the substantial and foreseeable risk of harm from a data breach, yet  
15 Defendant failed to properly prepare for that risk.

16 **H. The Data Breach Has and Will Continue to Cause Disruption and**  
17 **Increased Risk of Fraud and Identity Theft**

18 167. Cyberattacks and data breaches at mortgage companies like Defendant  
19 are especially problematic because they can negatively impact the overall daily lives  
20 of individuals affected by the attack.

21 168. The USGAO released a report in 2007 regarding data breaches ("GAO  
22 Report") in which it noted that victims of identity theft will face "substantial costs  
23 and time to repair the damage to their good name and credit record."<sup>56</sup>

24  
25 <sup>53</sup> David Lazarus, *Column: Shadowy data brokers make the most of their invisibility*  
26 *cloak*, Los Angeles Times (Nov. 5, 2019, 5:00 a.m. PT),  
<https://www.latimes.com/business/story/2019-11-05/column-data-brokers>.

27 <sup>54</sup> Datacoup, Inc. Home Page, <https://datacoup.com/> (last visited May 30, 2024).

28 <sup>55</sup> See <https://digi.me/what-is-digime/> (last visited May 30, 2024).

<sup>56</sup> *Supra*, n. 13.

1           169. That is because a data breach victim is exposed to serious ramifications  
2 regardless of the nature of the data. Indeed, the reason criminals steal Private  
3 Information is to monetize it. They do this by selling the spoils of their cyberattacks  
4 on the black market to identity thieves who desire to extort and harass victims, take  
5 over victims' identities in order to engage in illegal financial transactions under the  
6 victims' names. Because a person's identity is akin to a puzzle, the more accurate  
7 pieces of data an identity thief obtains about a person, the easier it is for the thief to  
8 take on the victim's identity, or otherwise harass or track the victim. For example,  
9 armed with just a name and date of birth, a data thief can utilize a hacking technique  
10 referred to as "social engineering" to obtain even more information about a victim's  
11 identity, such as a person's login credentials or SSN. Social engineering is a form of  
12 hacking whereby a data thief uses previously acquired information to manipulate  
13 individuals into disclosing additional confidential or personal information through  
14 means such as spam phone calls and text messages, or phishing emails.

15           170. The FTC recommends that identity theft victims take several steps to  
16 protect their personal and financial information after a data breach, including  
17 contacting one of the credit bureaus to place a fraud alert (or an extended fraud alert  
18 that lasts for 7 years if someone steals their identity), reviewing their credit reports,  
19 contacting companies to remove fraudulent charges from their accounts, placing a  
20 credit freeze on their credit, and correcting their credit reports.<sup>57</sup>

21           171. Identity thieves use stolen personal information such as SSNs for a  
22 variety of crimes, including credit card fraud, phone or utilities fraud, and  
23 bank/finance fraud.

24           172. Identity thieves can also use SSNs to obtain a driver's license or official  
25 identification card in the victim's name but with the thief's picture, use the victim's  
26 name and SSN to obtain government benefits, or file a fraudulent tax return using the

27 \_\_\_\_\_  
28 <sup>57</sup> *IdentityTheft.gov*, Federal Trade Commission, <https://www.identitytheft.gov/Steps>  
(last visited May 1, 2024).

1 victim's information. In addition, identity thieves may obtain a job using the victim's  
 2 SSN, rent a house or receive medical services in the victim's name, and may even  
 3 give the victim's personal information to police during an arrest resulting in an arrest  
 4 warrant being issued in the victim's name. Each of these fraudulent activities is  
 5 difficult to detect. An individual may not know that their SSN was used to file for  
 6 unemployment benefits until law enforcement notifies the individual's employer of  
 7 the suspected fraud. Fraudulent tax returns are typically discovered only when an  
 8 individual's authentic tax return is rejected.

9 173. Moreover, it is not an easy task to change, or cancel, a stolen SSN:

10 An individual cannot obtain a new Social Security number without  
 11 significant paperwork and evidence of actual misuse. Even then, a new  
 12 Social Security number may not be effective, as "[t]he credit bureaus and  
 13 banks are able to link the new number very quickly to the old number,  
 14 so all of that old bad information is quickly inherited into the new Social  
 15 Security number."<sup>58</sup>

16 174. In fact, as technology advances, computer programs may scan the  
 17 Internet with a wider scope to create a mosaic of information that may be used to link  
 18 compromised information to an individual in ways that were not previously possible.  
 19 This is known as the "mosaic effect."

20 175. One such example of criminals piecing together bits and pieces of  
 21 compromised Private Information for profit is the development of "Fullz" packages.<sup>59</sup>

22 <sup>58</sup> Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce*  
 23 *Back*, NPR (Feb. 9, 2015, 4:59 a.m. ET),

24 [http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-](http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft)  
 25 [millions-worrying-about-identity-theft.](http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft)

26 <sup>59</sup> "Fullz" is fraudster speak for data that includes the information of the victim,  
 27 including, but not limited to, the name, address, credit card information, SSN, date  
 28 of birth, and more. As a rule of thumb, the more information you have on a victim,  
 the more money that can be made from those credentials. Fullz are usually pricier  
 than standard credit card credentials, commanding up to \$100 per record (or more)  
 on the dark web. Fullz can be cashed out (turning credentials into money) in various

1           176. With “Fullz” packages, cyber-criminals can cross-reference two sources  
2 of Private Information to marry unregulated data available elsewhere to criminally  
3 stolen data with an astonishingly complete scope and degree of accuracy in order to  
4 assemble complete dossiers on individuals.

5           177. The development of “Fullz” packages means here that the stolen Private  
6 Information from the Data Breach can easily be used to link and identify it to  
7 Plaintiffs’ and Class Members’ phone numbers, email addresses, and other  
8 unregulated sources and identifiers. In other words, even if certain information such  
9 as emails, phone numbers, or credit card numbers may not be included in the Private  
10 Information that was exfiltrated in the Data Breach, criminals may still easily create  
11 a Fullz package and sell it at a higher price to unscrupulous operators and criminals  
12 (such as illegal and scam telemarketers) over and over.

13           178. The existence and prevalence of “Fullz” packages means that the Private  
14 Information stolen from the data breach can easily be linked to the unregulated data  
15 (like phone numbers and emails) of Plaintiffs and the other Class Members.

16           179. Thus, the information stolen in the Data Breach makes it easy for  
17 criminals to create a comprehensive “Fullz” package of Plaintiffs and Class Members,  
18 which can be sold and resold in perpetuity.

19 **V. PLAINTIFFS’ AND CLASS MEMBERS’ DAMAGES**

20           180. Numerous Plaintiffs have already suffered from actual misuse of the data  
21

22 \_\_\_\_\_  
23 ways, including performing bank transactions over the phone with the required  
24 authentication details in-hand. Even “dead Fullz,” which are Fullz credentials  
25 associated with credit cards that are no longer valid, can still be used for numerous  
26 purposes, including tax refund scams, ordering credit cards on behalf of the victim,  
27 or opening a “mule account” (an account that will accept a fraudulent money  
28 transfer from a compromised account) without the victim’s knowledge. *See, e.g.,*  
*Brian Krebs, Medical Records For Sale in Underground Stolen From Texas Life*  
*Insurance Firm*, Krebs on Security (Sep. 18, 2014, 10:40 a.m.),  
[https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-](https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm/)  
[stolen-from-texas-life-insurance-firm/](https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm/).

1 compromised in this Data Breach, and have suffered other concrete injuries (including  
2 lost time) as a result of that actual misuse.

3 181. As a direct and proximate cause of Defendant's Data Breach, Plaintiffs  
4 and Class Members face imminent, perpetual, and irreparable harm to their personal,  
5 financial, reputational, and future well-being.

6 182. Notably, there may be a substantial time lag—measured in years—  
7 between when harm occurs and when it is discovered, and also between when Private  
8 Information is stolen and when it is used. On average it takes approximately three  
9 months for consumers to discover their identity has been stolen and used, but it also  
10 sometimes takes years for others to learn that information.<sup>60</sup>

11 183. For example, the Social Security Administration has warned that identity  
12 thieves can use an individual's SSN to apply for additional credit lines.<sup>61</sup> Such fraud  
13 may go undetected until debt collection calls commence months, or even years, later.  
14 Stolen SSNs also make it possible for thieves to file fraudulent tax returns, file for  
15 unemployment benefits, or apply for a job using a false identity.<sup>62</sup> Each of these  
16 fraudulent activities is difficult to detect. An individual may not know that her or her  
17 SSN was used to file for unemployment benefits until law enforcement notifies the  
18 individual's employer of the suspected fraud. Fraudulent tax returns are typically  
19 discovered only when an individual's authentic tax return is rejected.

20 184. Based on the foregoing, the information compromised in the Data Breach  
21 is significantly more valuable than the loss of, for example, credit card information in  
22 a retailer data breach because, there, victims can cancel or close credit and debit card  
23 accounts. The information compromised in this Data Breach is impossible to "close"

24  
25 <sup>60</sup> John W. Coffey, Difficulties in Determining Data Breach Impacts, SYSTEMICS,  
26 CYBERNETICS AND INFORMATICS (2019),  
27 <http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf> (last visited May 1, 2024).

28 <sup>61</sup> *Identity Theft and Your Social Security Number*, Social Security Administration (July 2021), <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited May 30, 2024).

<sup>62</sup> *Id* at 4.

1 and difficult, if not impossible, to change, e.g., SSNs, addresses, and names.

2 185. This data, as one would expect, demands a much higher price on the  
3 black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained,  
4 “[c]ompared to credit card information, personally identifiable information and Social  
5 Security Numbers are worth more than 10x on the black market.”<sup>63</sup>

6 186. To date, Defendant has done little to provide Plaintiffs and the Class  
7 Members with relief for the damages they have suffered because of the Data Breach.

8 187. As a direct and proximate result of Defendant’s reckless and negligent  
9 actions, inaction, and omissions, the resulting Data Breach, the unauthorized release  
10 and disclosure of Plaintiffs’ and Class members’ Private Information, and  
11 Defendant’s failure to properly and timely notify Plaintiffs and Class members,  
12 Plaintiffs and Class members are more susceptible to identity theft and have  
13 experienced, will continue to experience and will face an increased risk of  
14 experiencing the following injuries, *inter alia*:

- 15 a. money and time expended to prevent, detect, contest, and repair  
16 identity theft, fraud, medical fraud, and/or other unauthorized uses  
17 of personal information;
- 18 b. money and time lost as a result of fraudulent access to and use of  
19 their accounts, including financial accounts;
- 20 c. loss of use of and access to their financial accounts and/or credit;
- 21 d. money and time expended to avail themselves of assets and/or credit  
22 frozen or flagged due to misuse;
- 23 e. impairment of their credit scores, ability to borrow, and/or ability to  
24 obtain credit;
- 25 f. lowered credit scores resulting from credit inquiries following  
26 fraudulent activities;

27  
28 <sup>63</sup> See, *supra*, n. 50.



- g. money, including fees charged in some states, and time spent placing fraud alerts and security freezes on their credit records;
- h. costs and lost time obtaining credit reports in order to monitor their credit records;
- i. anticipated future costs from the purchase of credit monitoring and/or identity theft protection services;
- j. costs and lost time from dealing with administrative consequences of the Data Breach, including by identifying, disputing, and seeking reimbursement for fraudulent activity, canceling compromised financial accounts and associated payment cards, and investigating options for credit monitoring and identity theft protection services;
- k. money and time expended to ameliorate the consequences of the filing of fraudulent tax returns;
- l. lost opportunity costs and loss of productivity from efforts to mitigate and address the adverse effects of the Data Breach including, but not limited to, efforts to research how to prevent, detect, contest, and recover from misuse of their personal information;
- m. loss of the opportunity to control how their Private Information is used; and
- n. continuing risks to their personal information, which remains subject to further harmful exposure and theft as long as Defendant fails to undertake appropriate, legally required steps to protect the personal information in its possession.

188. As a result of the events detailed herein, many victims have already suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach. This includes without limitation:

- reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;
- purchasing credit monitoring and identity theft prevention;
- placing “freezes” and “alerts” with reporting agencies;
- spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;
- contacting financial institutions and closing or modifying financial accounts; and
- closely reviewing and monitoring SSNs, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

189. Plaintiffs and Class Members have suffered and will continue to suffer from various forms of harm and privacy violations due the Data Breach, including but not limited to: invasion of privacy; loss of privacy; loss of control over personal information and identities; fraud and identity theft; unreimbursed losses relating to fraud and identity theft; loss of value and loss of possession and privacy of Personal Information; harm resulting from damaged credit scores and information; loss of time and money preparing for and resolving fraud and identity theft; loss of time and money obtaining protections against future identity theft; and other harm resulting from the unauthorized use or threat of unauthorized exposure of Private Information.

190. Plaintiffs and Class Members were also damaged in that they overpaid for a service that was intended to be accompanied by adequate data security that complied with industry standards but was not. Part of the price Plaintiffs and Class Members paid to Defendant was intended to be used by Defendant to fund adequate security of Defendant’s systems and Plaintiffs’ and Class Members’ Private Information. Thus, Plaintiffs and Class Members did not get what they paid for and agreed to, and were deprived of the benefit of their bargain.

191. Further, as a direct and proximate result of Defendant’s conduct, Plaintiffs and Class Members are forced to live with the fear, anxiety, and stress that

1 their Private Information may be disclosed at any moment to the entire world, thereby  
 2 subjecting them to embarrassment and depriving them of any right to privacy. This  
 3 emotional distress goes beyond allegations of mere worry or inconvenience—it is  
 4 exactly the sort of injury and harm to a data breach victim that the law contemplates  
 5 and addresses.

## 6 **VI. CLASS ACTION ALLEGATIONS**

7 192. Pursuant to Federal Rule of Civil Procedure 23, Plaintiffs bring this  
 8 action on behalf of themselves and on behalf of all other persons similarly situated.  
 9 Plaintiffs propose the following Nationwide Class and State Subclass definitions  
 10 (collectively the “Class”), subject to amendment as appropriate:

### 11 **Nationwide Class**

12 All persons in the United States whose data was impacted or otherwise  
 13 compromised by the Data Breach reported by loanDepot in January 2024,  
 14 including all those who were sent notice (the “Nationwide Class”).

### 15 **Arizona Subclass**

16 All persons in the state of Arizona whose data was impacted or otherwise  
 17 compromised by the Data Breach reported by loanDepot in January 2024,  
 18 including all those who were sent Notice (the “Arizona Subclass”).

### 19 **California Subclass**

20 All persons in the state of California whose data was impacted or otherwise  
 21 compromised by the Data Breach reported by loanDepot in January 2024,  
 22 including all those who were sent Notice (the “California Subclass”).

### 23 **Colorado Subclass**

24 All persons in the state of Colorado whose data was impacted or otherwise  
 25 compromised by the Data Breach reported by loanDepot in January 2024,  
 26 including all those who were sent Notice (the “Colorado Subclass”).

### 27 **Florida Subclass**

28 All persons in the state of Florida whose data was impacted or otherwise  
 29 compromised by the Data Breach reported by loanDepot in January 2024,  
 30 including all those who were sent Notice (the “Florida Subclass”).

### 31 **Illinois Subclass**

32 All persons in the state of Illinois whose data was impacted or otherwise  
 33 compromised by the Data Breach reported by loanDepot in January 2024,  
 34 including all those who were sent Notice (the “Illinois Subclass”).

1 compromised by the Data Breach reported by loanDepot in January 2024,  
2 including all those who were sent Notice (the “Illinois Subclass”).

3 **Maine Subclass**

4 All persons in the state of Maine whose data was impacted or otherwise  
5 compromised by the Data Breach reported by loanDepot in January 2024,  
6 including all those who were sent Notice (the “Maine Subclass”).

7 **New York Subclass**

8 All persons in the state of New York whose data was impacted or otherwise  
9 compromised by the Data Breach reported by loanDepot in January 2024,  
10 including all those who were sent Notice (the “New York Subclass”).

11 **North Carolina Subclass**

12 All persons in the state of North Carolina whose data was impacted or  
13 otherwise compromised by the Data Breach reported by loanDepot in January  
14 2024, including all those who were sent Notice (the “North Carolina  
15 Subclass”).

16 193. All members of the proposed Class are readily ascertainable. Defendant  
17 has access to Class Members’ names and addresses affected by the Data Breach.

18 194. Excluded from the Class are Defendant’s officers, directors; any entity  
19 in which Defendant has a controlling interest; and the affiliates, legal representatives,  
20 attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class  
21 are members of the judiciary to whom this case is assigned, their families and  
22 Members of their staff.

23 195. Plaintiffs reserve the right to amend or propose additional classes or  
24 subclasses upon conducting discovery.

25 196. This action is brought and may be properly maintained as a class action  
26 pursuant to Fed. R. Civ. P. 23(b)(2) and 23(b)(3), and satisfies the numerosity,  
27 commonality, typicality, adequacy, predominance, and superiority requirements of  
28 these rules.

197. **Numerosity.** The Members of the Class are so numerous that joinder of  
all of them is impracticable. The approximate number of Nationwide Class Members  
is 16.9 million. The exact number of members belonging to each Subclass is unknown  
to Plaintiffs at this time, based on information and belief and loanDepot’s public

1 disclosures, the Subclasses consists of millions of individuals whose sensitive data  
2 was compromised in the Data Breach.

3 198. **Commonality.** There are questions of law and fact common to the Class,  
4 which predominate over any questions affecting only individual Class Members.  
5 These common questions of law and fact include, without limitation:

- 6 • if Defendant unlawfully used, maintained, lost, or disclosed  
7 Plaintiffs' and Class Members' Private Information;
- 8 • if Defendant failed to implement and maintain reasonable  
9 security procedures and practices appropriate to the nature and  
10 scope of the information compromised in the Data Breach.
- 11 • if Defendant's data security systems prior to and during the Data  
12 Breach complied with applicable data security laws and  
13 regulations;
- 14 • if Defendant's data security systems prior to and during the Data  
15 Breach were consistent with industry standards;
- 16 • if Defendant owed a duty to Class Members to safeguard their  
17 Private Information;
- 18 • if Defendant breached their duty to Class Members to safeguard  
19 their Private Information;
- 20 • if Defendant knew or should have known that their data security  
21 systems and monitoring processes were deficient;
- 22 • if Defendant should have discovered the Data Breach sooner;
- 23 • if Plaintiffs and Class Members suffered legally cognizable  
24 damages as a result of Defendant's misconduct;
- 25 • if Defendant's conduct was negligent;
- 26 • if Defendant's breach implied contracts with Plaintiffs and Class  
27 Members;
- 28 • if Defendant were unjustly enriched by unlawfully retaining a  
benefit conferred upon them by Plaintiffs and Class Members;

//

- if Defendant failed to provide notice of the Data Breach in a timely manner; and
- if Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

199. **Typicality.** Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' information, like that of every other Class Member, was compromised in the Data Breach.

200. **Adequacy of Representation.** Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions.

201. **Predominance.** Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

202. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and

1 protects the rights of each Class Member.

2       203. **Declaratory and Injunctive Relief.** In addition, Defendant has acted  
3 and/or refused to act on grounds that apply generally to the Nationwide Class, making  
4 injunctive and/or declaratory relief appropriate with respect to the class under Federal  
5 Rule of Civil Procedure 23(b)(2). Defendant continues to (1) maintain the personally  
6 identifiable information of Nationwide Class Members, (2) fail to adequately protect  
7 Class Members' personally identifiable information, and (3) violate Class Members'  
8 rights under numerous state consumer protection laws and other claims alleged herein.  
9 Defendant has acted on grounds that apply generally to the Class as a whole, so that  
10 Class certification, injunctive relief, and corresponding declaratory relief are  
11 appropriate on a Class-wide basis.

12       204. Particular issues under Rule 42(d)(1) are also appropriate for certification  
13 because such claims present only particular, common issues, the resolution of which  
14 would advance the disposition of this matter and the parties' interests therein. Such  
15 particular issues were set forth above, and include, but are not limited to, whether  
16 Defendant failed to timely notify Plaintiffs and Class Members of the Data Breach,  
17 and whether Defendant's security measures were reasonable.

## 18 **VII. CHOICE OF LAW**

19       205. The loanDepot website Terms of Use state, "This Agreement and the  
20 resolution of any dispute related to this Agreement or this Site shall be governed by  
21 and construed in accordance with the laws of California without giving effect to any  
22 principles of conflicts of law," indicating loanDepot's intent to be governed by the  
23 laws of California in the procuring and management of loans.<sup>64</sup>

24       206. loanDepot elected to have California law govern all claims and disputes  
25 concerning the website at issue in this lawsuit. Accordingly, the application of  
26

---

27 <sup>64</sup> *Terms of Use*, loanDepot, <https://www.loandepot.com/termsfuse> (last visited June  
28 3, 2024).



1 California law to all of the Class Members' claims is fair, appropriate, and an election  
2 affirmatively made by loanDepot consistent in its agreements.

3 207. Beyond loanDepot's election of California law to govern the claims  
4 described herein, the State of California has a significant interest in regulating the  
5 conduct of businesses operating within its borders. California, which seeks to protect  
6 the rights and interests of California and all residents and citizens of the United States  
7 against a company headquartered and doing business in California, has a greater  
8 interest in the claims of Plaintiffs and class members than any other state or country  
9 and is most intimately concerned with the claims and outcome of this litigation.

10 208. The principal place of business of loanDepot, located at 6561 Irvine  
11 Center Drive, Irvine, California, is the "nerve center" of its business activities—the  
12 place where its high-level officers direct, control, and coordinate the corporation's  
13 activities, including its marketing, software development, and major policy, financial,  
14 and legal decisions.

15 209. loanDepot's response to the allegations herein, and corporate decisions  
16 surrounding such response, were made from and in California.

17 210. loanDepot's breaches of duty to Plaintiffs and the Class emanated from  
18 California, and the website at issue herein, on information and belief, was designed,  
19 created, and tested in California.

20 211. Application of California law with respect to Plaintiffs' and Class  
21 Members' claims is neither arbitrary nor fundamentally unfair because California has  
22 a state interest in the claims of the Plaintiffs and the Class based upon loanDepot's  
23 significant and ongoing contacts with California.

24 212. Under California's choice of law principles, which are applicable to this  
25 action, the common law of California applies to the common law claims of all class  
26 members. Additionally, given California's significant interest in regulating the  
27 conduct of businesses operating within its borders, California's consumer protection  
28 laws may be applied to non-resident Plaintiffs and class members.

**VIII. CAUSES OF ACTION**

**FIRST CAUSE OF ACTION**

**Negligence**

**(On Behalf of Plaintiffs and the Nationwide Class or, alternatively, the State Subclasses)**

213. Plaintiffs re-allege and incorporate by reference all other paragraphs of this complaint as though fully set forth herein.

214. Plaintiffs and the Class entrusted Defendant with their Private Information on the premise and with the understanding that Defendant would safeguard their information, use their Private Information for limited business purposes only, and/or not disclose their Private Information to unauthorized third parties.

215. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and the Class could and would suffer if the Private Information were wrongfully disclosed.

216. Defendant has a duty to Plaintiffs and Class Members to safeguard and protect their Private Information.

217. Defendant has a duty to use ordinary care in activities from which harm might be reasonably anticipated in connection with Private Information data.

218. By collecting and storing this data in its computer system and network, and sharing it and using it for commercial gain, Defendant owed a duty of care to use reasonable means to secure and safeguard its computer system – and Class Members’ Private Information held within it – to prevent disclosure of the information, and to safeguard the information. Defendant’s duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

219. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and all other requirements

1 discussed herein, and to ensure that its systems and networks, and the personnel  
2 responsible for them, adequately protected the Private Information.

3       220. Defendant's duty of care to use reasonable security measures arose  
4 because of the special relationship that existed between Defendant and individuals  
5 who entrusted them with Private Information, which is recognized by laws and  
6 regulations, as well as common law. Defendant was in a superior position to ensure  
7 that its systems were sufficient to protect against the foreseeable risk of harm to Class  
8 Members from a data breach.

9       221. Defendant's duty to use reasonable security measures required  
10 Defendant to reasonably protect confidential data from any intentional or  
11 unintentional use or disclosure.

12       222. Defendant breached its duty of care by failing to secure and safeguard  
13 the Private Information of Plaintiffs and Class Members. Defendant negligently  
14 stored and/or maintained its data security systems and published that information on  
15 the Internet.

16       223. Further, Defendant by and through its above negligent actions and/or  
17 inactions, breached its duties to Plaintiffs and Class Members by failing to design,  
18 adopt, implement, control, manage, monitor, and audit its processes, controls,  
19 policies, procedures, and protocols for complying with the applicable laws and  
20 safeguarding and protecting Plaintiffs' and Class Members' Private Information  
21 within its possession, custody and control.

22       224. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45),  
23 Defendant had a duty to provide adequate data security practices in connection with  
24 safeguarding Plaintiffs' and Class Members' Private Information.

25       225. Defendant breached its duties to Plaintiffs and Class Members under the  
26 Federal Trade Commission Act (15 U.S.C. § 45), the Gramm-Leach-Bliley Act (15  
27 U.S.C. §§ 6801, et seq.) ("GLBA"), the California Consumer Privacy Act, Cal. Civ.  
28 Code §§ 1798.100, et seq. ("CCPA"), Cal. Civ. Code §§ 1798.80, et seq., the

1 Consumers Legal Remedies Act, the Customer Record's Act, among other statutes,  
2 by failing to provide fair, reasonable, or adequate data security in connection with  
3 the sale of lending products and services in order to safeguard Plaintiffs' and Class  
4 Members' Private Information.

5 226. Plaintiffs and the other Class Members have suffered harm as a result of  
6 Defendant's negligence. These victims' loss of control over the compromised Private  
7 Information subjects each of them to a greatly enhanced risk of identity theft, fraud,  
8 and myriad other types of fraud and theft stemming from either the use of the  
9 compromised information or access to their user accounts.

10 227. It was reasonably foreseeable – in that Defendant knew or should have  
11 known – that its failure to exercise reasonable care in safeguarding and protecting  
12 Plaintiffs' and Class Members' Private Information would result in its release and  
13 disclosure to unauthorized third parties who, in turn, wrongfully used such Private  
14 Information, or disseminated it to other fraudsters for their wrongful use and for no  
15 lawful purpose.

16 228. But for Defendant's negligent and wrongful breach of its responsibilities  
17 and duties owed to Plaintiffs and Class Members, their Private Information would  
18 not have been compromised.

19 229. As a direct and proximate result of Defendant's above-described  
20 wrongful actions, inactions, and omissions, the resulting Data Breach, and the  
21 unauthorized release and disclosure of Plaintiffs' and Class Members' Private  
22 Information, they have incurred (and will continue to incur) the above-referenced  
23 economic damages, and other actual injury and harm for which they are entitled to  
24 compensation. Defendant's wrongful actions, inactions, and omissions constituted  
25 (and continue to constitute) common law negligence.

26 230. Plaintiffs and Class Members are entitled to injunctive relief as well as  
27 actual and punitive damages.  
28

**SECOND CAUSE OF ACTION**  
**Breach of Express Contract**  
**(On Behalf of Plaintiffs and the Nationwide Class Against Defendant or, alternatively, the State Subclasses)**

231. Plaintiffs re-allege and incorporate by reference all other paragraphs of this complaint as though fully set forth herein.

232. Plaintiffs and Class Members entered into a valid and enforceable contract through which they were required to turn over their sensitive personal information to Defendant in exchange for Defendant's services.

233. That contract included promises by Defendant to secure, safeguard, and not disclose Plaintiffs' and Class Members' sensitive personal information to any third parties without their consent.

234. Defendant's Privacy Policy memorialized the rights and obligations of Defendant and its customers. Defendant's Privacy Policy and/or the representations contained therein were provided to Plaintiffs and Class Members in a way that it became part of the agreement for services with Defendant.

235. Aside from state and federal laws, regulations, and industry standards, through the Privacy Policy, Defendant committed to protecting the privacy and security of the sensitive Private Information and promised to never share Plaintiffs' and Class Members' Private Information except under certain limited circumstances.

236. Plaintiffs and Class Members performed substantially all that was required of them under their contract with Defendant, or they were excused from doing so.

237. Defendant failed to perform its obligations under the contract, including by failing to provide adequate privacy, security, and confidentiality safeguards for Plaintiffs and Class Member's Private Information.

238. Defendant also violated the covenant of good faith and fair dealing by its conduct alleged herein.

1        239. Every contract has an implied covenant of good faith and fair dealing.  
 2 This implied covenant is an independent duty and may be breached even when there  
 3 is no breach of a contract's actual and/or express terms.

4        240. Plaintiffs and Class Members have complied with and performed all, or  
 5 substantially all, of the obligations imposed on their conditions with Defendant.

6        241. Defendant breached the implied covenant of good faith and fair dealing  
 7 by failing to maintain adequate computer systems and data security practices to  
 8 safeguard its customers' Private Information, failing to timely and accurately  
 9 disclose the Data Breach to Plaintiffs and Class Members and continued acceptance  
 10 of Private Information and storage of other personal information after Defendant  
 11 knew, or should have known, of the security vulnerabilities of the systems that were  
 12 exploited in the Data Breach.

13        242. Defendant breached the implied covenant of good faith and fair dealing  
 14 by, among other things:

- 15            • disclosing Plaintiffs' and other Class Members' personal  
 16 information to unauthorized third parties;
- 17            • allowing third parties to access the personal information of  
 18 Plaintiffs and other Class Members;
- 19            • failing to implement and maintain adequate security measures to  
 20 safeguard users' personal information;
- 21            • failing to timely notify Plaintiffs and other Class Members of the  
 22 unlawful disclosure of their personal information; and
- 23            • failing to maintain adequate security and proper encryption in  
 24 Defendant's websites, customer portals, and services.

25        243. As a direct and proximate result of Defendant's breach of contract, or its  
 26 independent breach of the implied covenant of good faith and fair dealing, Plaintiffs  
 27 and Class Members did not receive the benefit of the bargain, and instead, the  
 28 services they acquired from Defendant were less valuable than described in their  
 contracts. Plaintiffs and Class Members, therefore, were damaged in an amount at

1 least equal to the difference in value between that which was promised and  
2 Defendant's deficient performance.

3 244. Also, as a result of Defendant's breach of contract, or its independent  
4 breach of the implied covenant of good faith and fair dealing, Plaintiffs and Class  
5 Members have suffered actual damages resulting from the exposure of their Private  
6 Information, and they remain at imminent risk of suffering additional damages in the  
7 future.

8 245. Accordingly, Plaintiffs and Class Members have been injured by  
9 Defendant's breach of contract and are entitled to damages, including nominal  
10 damages, and/or restitution in an amount to be proven at trial.

11 **THIRD CAUSE OF ACTION**  
12 **Breach of Implied Contract**  
13 **(On Behalf of Plaintiffs and the Nationwide Class Against Defendant or,**  
14 **alternatively, the State Subclasses)**

15 246. Plaintiffs re-allege and incorporate by reference all other paragraphs of  
16 this complaint as though fully set forth herein.

17 247. Defendant provides mortgages, loans, or other financial services to  
18 Plaintiffs and Class Members. Plaintiffs and Class Members formed an implied  
19 contract with Defendant regarding the provision of those services through its  
20 collective conduct, including by Plaintiffs and Class Members providing their Private  
21 Information to Defendant in exchange for the services offered.

22 248. Through Defendant's offering of these lending and financial services, it  
23 knew or should have known that it needed to protect Plaintiffs' and Class Members'  
24 confidential Private Information in accordance with their own policies, practices, and  
25 applicable state and federal law.

26 249. As consideration, Plaintiffs and Class Members turned over valuable  
27 Private Information relying on Defendant to securely maintain and store their Private  
28 Information in return and in connection with their services.

//



1        250. Defendant accepted possession of Plaintiffs' and Class Members'  
2 Private Information for the purpose of providing its services, including data security,  
3 to Plaintiffs and Class Members.

4        251. In delivering their Private Information to Defendant in exchange for their  
5 services, Plaintiffs and Class Members intended and understood that Defendant  
6 would adequately safeguard their Private Information as part of those services.

7        252. Defendant's implied promises to Plaintiffs and Class Members include,  
8 but are not limited to, (1) taking steps to ensure that anyone who is granted access to  
9 Private Information, including its business associates, vendors, and/or suppliers, also  
10 protect the confidentiality of that data; (2) taking steps to ensure that the Private  
11 Information that is placed in the control of its business associates, vendors, and/or  
12 suppliers is restricted and limited to achieve an authorized business purpose; (3)  
13 restricting access to Private Information to qualified and trained employees, business  
14 associates, vendors, and/or suppliers; (4) designating and implementing appropriate  
15 retention policies to protect the Private Information against criminal data breaches;  
16 (5) applying or requiring proper encryption; and (6) taking other steps to protect  
17 against foreseeable data breaches.

18        253. Plaintiffs and Class Members would not have entrusted their Private  
19 Information to Defendant in the absence of such an implied contract.

20        254. Had Defendant disclosed to Plaintiffs and the Class that it did not have  
21 adequate data security and data supervisory practices to ensure the security of their  
22 sensitive data, including but not limited to Defendant's decision to continue to  
23 collect, store, and maintain Plaintiffs' and Class Members' Private Information  
24 despite knowledge of Defendant's previous data breach, Plaintiffs and Class  
25 Members would not have agreed to provide their Private Information to Defendant.

26        255. As providers of mortgage, lending, and financial services, Defendant  
27 recognized (or should have recognized) that Plaintiffs' and Class Member's Private  
28 Information is highly sensitive and must be protected, and that this protection was of

1 material importance as part of the bargain with Plaintiffs and the Class.

2 256. A meeting of the minds occurred, and an implied contract was formed,  
3 as Plaintiffs and Class Members agreed, *inter alia*, to provide their accurate and  
4 complete sensitive personal information to Defendant in exchange for Defendant's  
5 agreement to, *inter alia*, protect their Private Information.

6 257. Defendant violated these implied contracts by failing to employ  
7 reasonable and adequate security measures and supervision of its systems and  
8 networks, as well as its vendors, business associates, and/or suppliers, to secure  
9 Plaintiffs' and Class Members' Private Information.

10 258. Defendant also violated the covenant of good faith and fair dealing by its  
11 conduct alleged herein.

12 259. Every contract, including implied contracts, has an implied covenant of  
13 good faith and fair dealing. This implied covenant is an independent duty and may  
14 be breached even when there is no breach of a contract's actual and/or express terms.

15 260. Plaintiffs and Class Members have complied with and performed all, or  
16 substantially all, of the obligations imposed on their conditions with Defendant.

17 261. Defendant breached the implied covenant of good faith and fair dealing  
18 by failing to maintain adequate computer systems and data security practices to  
19 safeguard its customers' Private Information, failing to timely and accurately  
20 disclose the Data Breach to Plaintiffs and Class Members and continued acceptance  
21 of Private Information and storage of other personal information after Defendant  
22 knew, or should have known, of the security vulnerabilities of the systems that were  
23 exploited in the Data Breach.

24 262. Defendant breached the implied covenant of good faith and fair dealing  
25 by, among other things:

- 26 • disclosing Plaintiffs' and other Class Members' personal  
27 information to unauthorized third parties;
- 28 • allowing third parties to access the personal information of

1 Plaintiffs and other Class Members;

- 2 • failing to implement and maintain adequate security measures to
- 3 safeguard users' personal information;
- 4 • failing to timely notify Plaintiffs and other Class Members of the
- 5 unlawful disclosure of their personal information; and
- 6 • failing to maintain adequate security and proper encryption in
- 7 Defendant's websites, customer portals, and services.

8 263. Plaintiffs and Class Members have been damaged by Defendant's  
9 conduct, including the harms and injuries arising from the Data Breach now and in  
10 the future, as alleged herein.

11 264. Accordingly, Plaintiffs and Class Members have been injured by  
12 Defendant's breach of contract and are entitled to damages, including nominal  
13 damages, and/or restitution in an amount to be proven at trial.

#### 14 **FOURTH CAUSE OF ACTION**

##### **Invasion of Privacy**

15 **(On Behalf of Plaintiffs and the Nationwide Class Against Defendant, or,**  
16 **alternatively, Plaintiffs Krieghauser, Isaiah, and Singh and the California**  
17 **Subclass)**

18 265. Plaintiffs re-allege and incorporate by reference all other paragraphs of  
19 this complaint as though fully set forth herein.

20 266. Plaintiffs bring this claim on behalf of themselves and the Nationwide  
21 Class and the Nationwide Class, or, alternatively, California Plaintiffs Krieghauser,  
22 Isaiah, and Singh and the California Subclass.

23 267. Plaintiffs and Class Members had a legally protected privacy interest and  
24 a reasonable expectation of privacy in the Private Information that Defendant  
25 required them to provide, stored, and mishandled.

26 268. California established the right to privacy in Article 1, Section 1 of the  
27 California Constitution.

28 269. The State of California recognizes the tort of Intrusion into Private  
Affairs, and adopts the formulation of that tort found in the Restatement (Second) of

1 Torts which states:

2 One who intentionally intrudes, physically or otherwise,  
3 upon the solitude or seclusion of another or his private  
4 affairs or concerns, is subject to liability to the other for  
5 invasion of his privacy, if the intrusion would be highly  
6 offensive to a reasonable person. Restatement (Second) of  
7 Torts § 652B (1977).

8 270. Plaintiffs and Class Members reasonably expected that their Private  
9 Information would be protected and secured from unauthorized parties, would not be  
10 disclosed to any unauthorized parties or disclosed for any improper purpose.

11 271. Defendant owed a duty to customers in its network, including Plaintiffs  
12 and Class members, to keep their Private Information confidential.

13 272. The unauthorized release of Private Information is highly offensive to a  
14 reasonable person.

15 273. Defendant unlawfully invaded the privacy rights of Plaintiffs and Class  
16 Members by (a) failing to adequately secure their Private Information from  
17 disclosure to unauthorized parties for improper purposes; (b) disclosing their Private  
18 Information to unauthorized parties in a manner that is highly offensive to a  
19 reasonable person; and (c) disclosing their Private Information to unauthorized  
20 parties without the informed and clear consent of Plaintiffs and Class Members. This  
21 invasion into the privacy interest of Plaintiffs and Class Members is serious and  
22 substantial.

23 274. In failing to adequately secure Plaintiffs' and Class Members' Private  
24 Information, Defendant acted in reckless disregard of their privacy rights. Defendant  
25 knew or should have known that its substandard security measures would cause its  
26 users harm and, would be considered highly offensive to a reasonable person in the  
27 same position as Plaintiffs and Class Members.

28 275. Defendant violated Plaintiffs' and Class Members' right to privacy under  
California law, including, but not limited to California common law and Article 1,  
Section 1 of the California Constitution and the California Consumer Privacy Act.

1           276. Defendant's conduct as alleged above intruded upon Plaintiffs and Class  
2 Members' seclusion under common law.

3           277. By intentionally failing to keep Plaintiffs' and Class Members' Private  
4 Information safe, and by intentionally misusing and/or disclosing said information to  
5 unauthorized parties for unauthorized use, Defendant intentionally invaded Plaintiffs  
6 and Class Members' privacy by:

- 7           • Intentionally and substantially intruding into Plaintiffs and Class  
8 Members' private affairs in a manner that identifies Plaintiffs and Class  
9 Members and that would be highly offensive and objectionable to an  
ordinary person;
- 10          • Intentionally publicizing private facts about Plaintiffs and Class  
11 Members, which is highly offensive and objectionable to an ordinary  
12 person; and
- 13          • Intentionally causing anguish or suffering to Plaintiffs and Class  
14 Members.

15           278. Defendant acted with a knowing state of mind when it permitted the Data  
16 Breach because it knew its information security practices were inadequate and would  
17 likely result in a data breach such as the one that harmed Plaintiffs and Class  
18 members.

19           279. Defendant knew that an ordinary person in Plaintiffs or Class Members'  
20 position would consider Defendant's intentional actions highly offensive and  
21 objectionable.

22           280. Defendant invaded Plaintiffs and Class Members' right to privacy and  
23 intruded into Plaintiffs' and Class Members' private affairs by misusing and/or  
24 disclosing their Private Information without their informed, voluntary, affirmative,  
25 and clear consent.

26           281. Defendant concealed from and delayed reporting to Plaintiffs and Class  
27 Members the Data Breach that misused and/or disclosed their Private Information  
28 without their informed, voluntary, affirmative, and clear consent.

1        282. The conduct described above was directed at Plaintiffs and Class  
2 Members.

3        283. As a proximate result of such intentional misuse and disclosures,  
4 Plaintiffs' and Class Members' reasonable expectations of privacy in their Private  
5 Information was unduly frustrated and thwarted. Defendant's conduct amounted to a  
6 substantial and serious invasion of Plaintiffs' and Class Members' protected privacy  
7 interests, causing anguish and suffering such that an ordinary person would consider  
8 Defendant's intentional actions or inaction highly offensive and objectionable.

9        284. In failing to protect Plaintiffs' and Class Members' Private Information,  
10 and in misusing and/or disclosing their Private Information, Defendant acted with  
11 intentional malice and oppression and in conscious disregard of Plaintiffs and Class  
12 Members' rights to have such information kept confidential and private. Plaintiffs,  
13 therefore, seek an award of damages on behalf themselves and the Class.

14        285. As a direct and proximate result of Defendant's conduct, Plaintiffs and  
15 Class Members are entitled to damages, including compensatory, punitive, and/or  
16 nominal damages, in an amount to be proven at trial.

17        286. As a direct and proximate result of Defendant's unlawful invasions of  
18 privacy, Plaintiffs' and Class Members' Private Information has been accessed, and  
19 their reasonable expectations of privacy have been intruded upon and frustrated.  
20 Plaintiffs and proposed Class Members have suffered injuries as a result of  
21 Defendant's unlawful invasions of privacy and are entitled to appropriate relief.

22        287. Plaintiffs and Class Members are entitled to injunctive relief as well as  
23 actual and punitive damages.

24                                    **FIFTH CAUSE OF ACTION**  
25                                    **Violations of the California Consumer Privacy Act**  
26                                    **California Civil Code § 1798.150**  
27                                    **(On Behalf of Plaintiffs and the Nationwide Class Against Defendant, or,**  
28                                    **alternatively, Plaintiffs Krieghauser, Isaiah, and Singh and the California**  
   **Subclass)**

28        288. Plaintiffs re-allege and incorporate by reference all other paragraphs of

1 this complaint as though fully set forth herein.

2 289. Plaintiffs bring this claim on behalf of themselves and the Nationwide  
3 Class and the Nationwide Class, or, alternatively, California Plaintiffs Krieghauser,  
4 Isaiah, and Singh and the California Subclass.

5 290. Cal. Civ. Code § 1798.150(a) of the California Consumer Privacy Act  
6 (“CCPA”) provides that “[a]ny consumer whose nonencrypted and nonredacted  
7 personal information, as defined in subparagraph (A) of paragraph (1) of subdivision  
8 (d) of Section 1798.81.5 . . . is subject to an unauthorized access and exfiltration, theft,  
9 or disclosure as a result of the business’s violation of the duty to implement and  
10 maintain reasonable security procedures and practices appropriate to the nature of the  
11 information to protect the personal information may institute a civil action” for  
12 statutory damages, actual damages, injunctive relief, declaratory relief and any other  
13 relief the court deems proper.

14 291. Defendant violated California Civil Code § 1798.150 of the CCPA by  
15 failing to implement and maintain reasonable security procedures and practices  
16 appropriate to the nature of the information to protect the nonencrypted Private  
17 Information of Plaintiffs and the Class. As a direct and proximate result, Plaintiffs’  
18 and the Class’s nonencrypted and nonredacted Private Information was subject to  
19 unauthorized access and exfiltration, theft, or disclosure.

20 292. Defendant is a “business” under the meaning of Civil Code § 1798.140  
21 because Defendant is a “corporation, association, or other legal entity that is organized  
22 or operated for the profit or financial benefit of its shareholders or other owners” that  
23 “collects consumers’ personal information” and is active “in the State of California”  
24 and “had annual gross revenues in excess of twenty-five million dollars (\$25,000,000)  
25 in the preceding calendar year.” Civil Code § 1798.140(d).

26 293. Plaintiffs and California Subclass Members are “consumers” as defined  
27 by Cal. Civ. Code § 1798.140(g) because they are natural persons who reside in  
28 California.



1           294. Plaintiffs and Class Members seek injunctive or other equitable relief to  
2 ensure Defendant hereinafter adequately safeguards Private Information by  
3 implementing reasonable security procedures and practices. Such relief is particularly  
4 important because Defendant continues to hold Private Information, including  
5 Plaintiffs' and Class Members' Private Information.

6           295. Plaintiffs and Class Members have an interest in ensuring that their  
7 Private Information is reasonably protected, and Defendant has demonstrated a  
8 pattern of failing to adequately safeguard this information.

9           296. Defendant has long had notice of Plaintiffs' allegations, claims and  
10 demands, including from the filing of numerous related actions against it arising from  
11 the Data Breach, the first of which were filed on or about January 19, 2024. Further,  
12 Defendant is the party with the most knowledge of the underlying facts giving rise to  
13 Plaintiffs' allegations, so that any pre-suit notice would not put Defendant in a better  
14 position to evaluate those claims. Plaintiffs further sent Defendant notice consistent  
15 with the CCPA on or before May 3, 2024. Based on information and belief, additional  
16 plaintiffs in related actions further provided Defendant with CCPA notice beginning  
17 on or about February 5, 2024.

18           297. Defendant failed to take sufficient and reasonable measures to safeguard  
19 its data security systems and protect Plaintiffs' and California Subclass Members'  
20 highly sensitive personal information and medical data from unauthorized access.  
21 Defendant's failure to maintain adequate data protections subjected Plaintiffs' and the  
22 California Subclass Members' nonencrypted and nonredacted sensitive personal  
23 information to exfiltration and disclosure by malevolent actors.

24           298. The unauthorized access, exfiltration, theft, and disclosure of Plaintiffs  
25 and the California Subclass Members' Private Information was a result of Defendant's  
26 violation of its duty to implement and maintain reasonable security procedures and  
27 practices appropriate to the nature of the information to protect the personal  
28 information.

300. Plaintiffs and California Subclass Members have suffered actual injury and are entitled to damages in an amount to be proven at trial but in excess of the minimum jurisdictional requirement of this Court.

302. Plaintiffs and California Subclass Members seek all monetary and non-monetary relief allowed by law, including actual or nominal damages; declaratory and injunctive relief, including an injunction barring Defendant from disclosing their PHI/Private Information without their consent; reasonable attorneys' fees and costs; and any other relief that is just and proper.

20 **SIXTH CAUSE OF ACTION**  
21 **Violations of the California Unfair Competition Law**  
**Cal. Bus. & Prof. Code § 17200, *et seq.* (“UCL”)**  
22 **(On Behalf of Plaintiffs and the Nationwide Class Against Defendant, or,**  
**alternatively, California Plaintiffs Kriehauser, Isaiah, and Singh and the**  
**California Subclass)**

305. Plaintiffs bring this claim on behalf of themselves and the Nationwide Class and the Nationwide Class, or, alternatively, California Plaintiffs Krieghauser, Isaiah, and Singh and the California Subclass.

1        306. The California Unfair Competition Law, Cal. Bus. & Prof. Code §17200,  
2 et seq. (“UCL”), prohibits any “unlawful,” “fraudulent” or “unfair” business act or  
3 practice and any false or misleading advertising, as defined by the UCL and relevant  
4 case law.

5        307. By reason of Defendant’s above-described wrongful actions, inactions,  
6 and omissions, the resulting Data Breach, and the unauthorized disclosure of  
7 Plaintiffs’ and Class members’ Private Information, Defendant engaged in unfair,  
8 unlawful, and fraudulent business practices in violation of the UCL.

9        308. The acts, omissions, and conduct complained of herein in violation of  
10 the UCL were designed and emanated from Defendant’s California corporate office.

11        309. Plaintiffs suffered injury, in fact, and lost money or property as a result  
12 of Defendant’s alleged violations of the UCL.

13        310. The acts, omissions, and conduct of Defendant as alleged herein  
14 constitute a “business practice” within the meaning of the UCL.

15 **Unlawful Prong**

16        311. Defendant violated the unlawful prong of the UCL by violating, inter  
17 alia, the CCPA, CCRA, GLBA, and FTC Act as alleged herein.

18        312. Defendant violated the unlawful prong of the UCL by failing to honor  
19 the terms of its implied contracts with Plaintiffs and Class Members, as alleged  
20 herein.

21        313. Defendant’s conduct also undermines California public policy—as  
22 reflected in statutes like the California Information Practices Act, Cal. Civ. Code §§  
23 1798, et seq., the CCPA concerning consumer privacy, and the CCRA concerning  
24 customer records—which seek to protect customer and consumer data and ensure  
25 that entities who solicit or are entrusted with personal data utilize reasonable security  
26 measures.

27 //

28 //

1 **Unfair Prong**

2 314. Defendant's acts, omissions, and conduct also violate the unfair prong of  
 3 the UCL because Defendant's acts, omissions, and conduct, as alleged herein,  
 4 offended public policy and constitute immoral, unethical, oppressive, and  
 5 unscrupulous activities that caused substantial injury, including to Plaintiffs and  
 6 other Class Members. The gravity of Defendant's conduct outweighs any potential  
 7 benefits attributable to such conduct and there were reasonably available alternatives  
 8 to further Defendant's legitimate business interests, other than Defendant's conduct  
 9 described herein.

10 315. Defendant's failure to utilize, and to disclose that it does not utilize,  
 11 industry standard security practices, constitutes an unfair business practice under the  
 12 UCL. Defendant's conduct is unethical, unscrupulous, and substantially injurious to  
 13 the Class. While Defendant's competitors have spent the time and money necessary  
 14 to appropriately safeguard their products, service, and customer information,  
 15 Defendant has not—to the detriment of its customers and to competition.

16 **Fraudulent Prong**

17 316. By failing to disclose that it does not enlist industry-standard security  
 18 practices, all of which rendered Class Members particularly vulnerable to data  
 19 breaches, Defendant engaged in UCL-violative practices.

20 317. A reasonable consumer would not have transacted with Defendant if they  
 21 knew the truth about its security procedures. By withholding material information  
 22 about its security practices, Defendant was able to obtain customers who provided  
 23 and entrusted their Personal Information in connection with transacting business with  
 24 Defendant. Had Plaintiffs known the truth about Defendant's security procedures,  
 25 Plaintiffs would not have done business with Defendant.

26 318. As a result of Defendant's violations of the UCL, Plaintiffs and Class  
 27 Members are entitled to injunctive relief including, but not limited to: (1) ordering  
 28 that Defendant utilize strong industry standard data security measures for the

1 collection, storage, and retention of customer data; (2) ordering that Defendant,  
2 consistent with industry standard practices, engage third party security  
3 auditors/penetration testers as well as internal security personnel to conduct testing,  
4 including simulated attacks, penetration tests, and audits on Defendant's systems on  
5 a periodic basis; (3) ordering that Defendant engage third party security auditors and  
6 internal personnel, consistent with industry standard practices, to run automated  
7 security monitoring; (4) ordering that Defendant audit, test, and train its security  
8 personnel regarding any new or modified procedures; (5) ordering that Defendant,  
9 consistent with industry standard practices, segment consumer data by, among other  
10 things, creating firewalls and access controls so that if one area of Defendant's  
11 systems are compromised, hackers cannot gain access to other portions of those  
12 systems; (6) ordering that Defendant purge, delete, and destroy in a reasonably secure  
13 manner Class member data not necessary for its provisions of services; (7) ordering  
14 that Defendant, consistent with industry standard practices, conduct regular database  
15 scanning and security checks; (8) ordering that Defendant, consistent with industry  
16 standard practices, evaluate all software, systems, or programs utilized for collection  
17 and storage of sensitive Private Information for vulnerabilities to prevent threats to  
18 customers; (9) ordering that Defendant, consistent with industry standard practices,  
19 periodically conduct internal training and education to inform internal security  
20 personnel how to identify and contain a breach when it occurs and what to do in  
21 response to a breach; and (10) ordering Defendant to meaningfully educate its  
22 customers about the threats they face as a result of the loss of their Private  
23 Information.

24 319. As a result of Defendant's violations of the UCL, Plaintiffs and Class  
25 Members have suffered injury in fact and lost money or property, as detailed herein.  
26 They agreed to transact with Defendant or made purchases or spent money that they  
27 otherwise would not have made or spent, had they known the true state of affairs  
28 regarding Defendant's data security policies. Class Members lost control over their

1 Private Information and suffered a corresponding diminution in value of that Private  
 2 Information, which is a property right. Class Members lost money as a result of  
 3 dealing with the fallout of and attempting to mitigate harm arising from the Data  
 4 Breach.

5 320. Plaintiffs request that the Court issue sufficient equitable relief to restore  
 6 Class Members to the position they would have been in had Defendant not engaged  
 7 in violations of the UCL, including by ordering restitution of all funds that Defendant  
 8 may have acquired from Plaintiffs and Class Members as a result of those violations.

9 **SEVENTH CAUSE OF ACTION**  
 10 **Violations of the California Consumer Records Act**  
 11 **Cal. Civ. Code § 1798.80, *et seq.* (“CCRA”)**  
 12 **(On Behalf of Plaintiffs and the Nationwide Class Against Defendant, or,**  
 13 **alternatively, California Plaintiffs Krieghauser, Isaiah, and Singh and the**  
 14 **California Subclass)**

13 321. Plaintiffs re-allege and incorporate by reference all other paragraphs of  
 14 this complaint as though fully set forth herein.

15 322. Plaintiffs bring this claim on behalf of themselves and the Nationwide  
 16 Class and the Nationwide Class, or, alternatively, California Plaintiffs Krieghauser,  
 17 Isaiah, and Singh and the California Subclass.

18 323. Under the California Consumer Records Act, any “person or business  
 19 that conducts business in California, and that owns or licenses computerized data that  
 20 includes personal information” must “disclose any breach of the system following  
 21 discovery or notification of the breach in the security of the data to any resident of  
 22 California whose unencrypted personal information was, or is reasonably believed to  
 23 have been, acquired by an unauthorized person.” Cal. Civ. Code §1798.82. The  
 24 disclosure must “be made in the most expedient time possible and without  
 25 unreasonable delay” but disclosure must occur “immediately following discovery [of  
 26 the breach], if the personal information was, or is reasonably believed to have been,  
 27 acquired by an unauthorized person.” *Id.* (emphasis added).

28 //

1           324. The Data Breach constitutes a “breach of the security system” of  
2 Defendant. An unauthorized person acquired the personal, unencrypted information  
3 of Plaintiffs and Class Members.

4           325. Defendant knew that an unauthorized person had acquired the personal,  
5 unencrypted information of Plaintiffs and the Class but waited to notify them. Given  
6 the severity of the Data Breach, this is an unreasonable delay.

7           326. Defendant’s unreasonable delay prevented Plaintiffs and the Class from  
8 taking appropriate measures from protecting themselves against harm.

9           327. As a direct or proximate result of Defendant’s violations of Civil Code  
10 §§ 1798.81.5 and 1798.82, Plaintiffs and Class Members were (and continue to be)  
11 injured and have suffered (and will continue to suffer) the damages and harms  
12 described herein.

13           328. Plaintiffs accordingly requests that the Court enter an injunction  
14 requiring Defendant to implement and maintain reasonable security procedures,  
15 including, but not limited to: (1) ordering that Defendant utilize strong industry  
16 standard data security measures for the collection, storage, and retention of customer  
17 data; (2) ordering that Defendant, consistent with industry standard practices, engage  
18 third-party security auditors/penetration testers as well as internal security personnel  
19 to conduct testing, including simulated attacks, penetration tests, and audits on  
20 Defendant’s systems on a periodic basis; (3) ordering that Defendant engage third  
21 party security auditors and internal personnel, consistent with industry standard  
22 practices, to run automated security monitoring; (4) ordering that Defendant audit,  
23 test, and train its security personnel regarding any new or modified procedures; (5)  
24 ordering that Defendant, consistent with industry standard practices, segment  
25 consumer data by, among other things, creating firewalls and access controls so that  
26 if one area of Defendant’s systems are compromised, hackers cannot gain access to  
27 other portions of those systems; (6) ordering that Defendant purge, delete, and  
28 destroy in a reasonably secure manner Class member data not necessary for its



1 provisions of services; (7) ordering that Defendant, consistent with industry standard  
 2 practices, conduct regular database scanning and security checks; (8) ordering that  
 3 Defendant, consistent with industry standard practices, evaluate all software,  
 4 systems, or programs utilized for collection and storage of sensitive Private  
 5 Information for vulnerabilities to prevent threats to customers; (9) ordering that  
 6 Defendant, consistent with industry standard practices, periodically conduct internal  
 7 training and education to inform internal security personnel how to identify and  
 8 contain a breach when it occurs and what to do in response to a breach; and (10)  
 9 ordering Defendant to meaningfully educate its customers about the threats they face  
 10 as a result of the loss of their Private Information.

11 329. Plaintiffs and Class Members seek relief under section 1798.84 of the  
 12 California Civil Code including, but not limited to, actual damages, to be proven at  
 13 trial, and injunctive relief.

14  
 15 **EIGHTH CAUSE OF ACTION**  
**Violations of the California Consumer Legal Remedies Act**  
**Remedies Act, California Civil Code § 1750, *et seq.***  
 16 **(On Behalf of Plaintiffs and the Nationwide Class Against Defendant, or,**  
 17 **alternatively, California Plaintiffs Krieghauser, Isaiah, and Singh and the**  
**California Subclass)**

18 330. Plaintiffs re-allege and incorporate by reference all other paragraphs of  
 19 this complaint as though fully set forth herein.

20 331. Plaintiffs bring this claim on behalf of themselves and the Nationwide  
 21 Class and the Nationwide Class, or, alternatively, California Plaintiffs Krieghauser,  
 22 Isaiah, and Singh and the California Subclass.

23 332. This cause of action is brought pursuant to the California Consumers  
 24 Legal Remedies Act (the “CLRA”), California Civil Code § 1750, *et seq.*

25 333. Defendant has long had notice of Plaintiffs’ allegations, claims and  
 26 demands, including from the filing of numerous related actions against it arising from  
 27 the Data Breach, the first of which were filed on or about January 19, 2024. Further,  
 28 Defendant is the party with the most knowledge of the underlying facts giving rise to

1 Plaintiffs’ allegations, so that any pre-suit notice would not put Defendant in a better  
2 position to evaluate those claims. Plaintiffs further sent Defendant notice consistent  
3 with the CLRA on or before May 3, 2024. Based on information and belief, additional  
4 plaintiffs in related actions further provided Defendant with CLRA notice beginning  
5 on or about February 5, 2024.

6 334. To the extent the Court finds Plaintiffs have still not met the CLRA  
7 notice requirements, Plaintiffs in the alternative seek only injunctive relief pursuant  
8 to Cal. Civ. Code § 1782, subdivision (d), which provides that “[a]n action for  
9 injunctive relief brought under the specific provisions of Section 1770 may be  
10 commenced without compliance with subdivision (a).”

11 335. Plaintiffs and Nationwide Class Members are “consumers,” as the term  
12 is defined by California Civil Code § 1761(d).

13 336. Plaintiffs, Nationwide Class Members, and Defendant have engaged in  
14 “transactions,” as that term is defined by California Civil Code § 1761(e).

15 337. The conduct alleged in this Complaint constitutes unfair methods of  
16 competition and unfair and deceptive acts and practices for the purpose of the CLRA,  
17 and the conduct was undertaken by Defendant was likely to deceive consumers.

18 338. Cal. Civ. Code § 1770(a)(5) prohibits one who is involved in a  
19 transaction from “[r]epresenting that goods or services have sponsorship, approval,  
20 characteristics, ingredients, uses, benefits, or quantities which they do not have.”

21 339. Defendant violated this provision by representing that it took appropriate  
22 measures to protect Plaintiffs’ and the Nationwide Class Members’ Private  
23 Information.

24 340. Additionally, Defendant improperly handled, stored, or protected either  
25 unencrypted or partially encrypted data.

26 341. As a result, Plaintiffs and Nationwide Class Members were induced to  
27 enter into a relationship with Defendant and provide their Private Information.

28 //

1           342. Defendant intended to, and did, mislead Plaintiffs and Class Members  
2 and induced them to rely on its misrepresentations and omissions.

3           343. Had Defendant disclosed to Plaintiffs and Class Members that its data  
4 systems were not secure and, thus, vulnerable to attack, Defendant would have been  
5 unable to continue in business and it would have been forced to adopt reasonable  
6 data security measures and comply with the law. Instead, Defendant received,  
7 maintained, and compiled Plaintiffs' and Class Members' Private Information as part  
8 of the services Defendant provided and for which Plaintiffs and Class Members paid  
9 without advising Plaintiffs and Class Members that Defendant's data security  
10 practices were insufficient to maintain the safety and confidentiality of Plaintiffs'  
11 and Class Members' Private Information. Accordingly, Plaintiffs and the Class  
12 Members acted reasonably in relying on Defendant's misrepresentations and  
13 omissions, the truth of which they could not have discovered.

14           344. As a result of engaging in such conduct, Defendant has violated Civil  
15 Code § 1770.

16           345. Pursuant to Civil Code § 1780(a)(2) and (a)(5), Plaintiffs seek an order  
17 of this Court that includes, but is not limited to, an order enjoining Defendant from  
18 continuing to engage in unlawful, unfair, or fraudulent business practices or any other  
19 act prohibited by law.

20           346. Plaintiffs and Class Members suffered injuries caused by Defendant's  
21 misrepresentations, because they provided their Private Information believing that  
22 Defendant would adequately protect this information.

23           347. Plaintiffs and Class Members may be irreparably harmed and/or denied  
24 an effective and complete remedy if such an order is not granted.

25           348. The unfair and deceptive acts and practices of Defendant, as described  
26 above, present a serious threat to Plaintiffs and Class Members.

27           349. Plaintiffs seek prospective injunctive relief, including improvements to  
28 Defendant's data security systems and practices, in order to ensure that such security

1 is reasonably sufficient to safeguard customers' Private Information that remains in  
2 Defendant's custody, including but not limited to the following:

- 3 A. Ordering that Defendant engage third-party security  
4 auditors/penetration testers as well as internal security personnel to  
5 conduct testing, including simulated attacks, penetration tests, and  
6 audits on Defendant's systems on a periodic basis, and ordering  
7 Defendant to promptly correct any problems or issues detected by  
8 such third-party security auditors;
- 9 B. Ordering that Defendant engage third-party security auditors and  
10 internal personnel to run automated security monitoring;
- 11 C. Ordering that Defendant audit, test, and train their security personnel  
12 regarding any new or modified procedures;
- 13 D. Ordering that Defendant segment customer data by, among other  
14 things, creating firewalls and access controls so that if one area of  
15 Defendant's systems is compromised, hackers cannot gain access to  
16 other portions of Defendant's systems;
- 17 E. Ordering that Defendant not transmit Private Information via  
18 unencrypted email;
- 19 F. Ordering that Defendant not store Private Information in email  
20 accounts;
- 21 G. Ordering that Defendant purge, delete, and destroy in a reasonably  
22 secure manner customer data not necessary for provisions of  
23 Defendant's services;
- 24 H. Ordering that Defendant conduct regular computer system scanning  
25 and security checks;
- 26 I. Ordering that Defendant routinely and continually conduct internal  
27 training and education to inform internal security personnel how to  
28 identify and contain a breach when it occurs and what to do in

1 response to a breach; and

2 J. Ordering Defendant to meaningfully educate their current, former,  
3 and prospective customers about the threats they face as a result of  
4 the loss of their Private Information to third parties, as well as the  
5 steps they must take to protect themselves.

6 350. Unless such Class-wide injunctive relief is issued, Plaintiffs and Class  
7 Members remain at risk, and there is no other adequate remedy at law that would  
8 ensure that Plaintiffs (and other consumers) can rely on Defendant's representations  
9 regarding its data security in the future.

10 351. Furthermore, in the alternative to all legal remedies sought herein,  
11 Plaintiffs, on behalf of the Class, seek monetary relief including but not limited to all  
12 damages recoverable under the CLRA, including, but not limited to, restitution to  
13 Plaintiffs and Class Members of money or property that Defendant may have  
14 acquired by means of Defendant's unlawful, and unfair business practices;  
15 restitutionary disgorgement of all profits accruing to Defendant because of  
16 Defendant's unlawful and unfair business practices; declaratory relief; and attorneys'  
17 fees and costs pursuant to Cal. Code Civ. Proc. § 1021.5.

18  
19 **NINTH CAUSE OF ACTION**  
20 **Violations of the Florida Deceptive and Unfair Trade Practices Act**  
21 **Fla. Stat. § 501.201, *et. seq.***  
**(On Behalf of Plaintiff Jessica Schuler and the Florida Subclass Against**  
**Defendant)**

22 352. Plaintiff Jessica Schuler ("Plaintiff" for the purposes of this count) re-  
23 alleges and incorporates by reference all other paragraphs of this complaint as though  
24 fully set forth herein and brings this claim on behalf of herself and the Florida  
25 Subclass (the "Class" for the purposes of this count).

26 353. Defendant engaged in the conduct alleged in this Complaint through  
27 transactions in and involving trade and commerce. Mainly, Defendant obtained  
28 Plaintiff's and the Class Members' Private Information through advertising,

1 soliciting, providing, offering, and/or distributing goods and services to Plaintiff and  
 2 the Class Members and the Data Breach occurred through the use of the internet, an  
 3 instrumentality of interstate commerce.

4 354. As alleged herein this Complaint, Defendant engaged in unfair or  
 5 deceptive acts or practices in the conduct of consumer transactions, including, among  
 6 other things, the following:

- 7 • failure to implement adequate data security practices to safeguard  
 8 Plaintiff's and Class Members' Private Information;
- 9 • failure to make only authorized disclosures of customers' and  
 10 applicants' Private Information;
- 11 • failure to disclose that their data security practices were  
 12 inadequate to safeguard customers' Private Information from  
 13 theft; and
- 14 • failure to timely and accurately disclose the Data Breach to  
 Plaintiff and Class Members.

15 355. Defendant's actions constitute unconscionable, deceptive, or unfair acts  
 16 or practices because, as alleged herein, Defendant engaged in immoral, unethical,  
 17 oppressive, and unscrupulous activities that are and were substantially injurious to  
 18 Defendant's current and former customers and/or applicants.

19 356. In committing the acts alleged above, Defendant engaged in  
 20 unconscionable, deceptive, and unfair acts and practices by omitting, failing to  
 21 disclose, or inadequately disclosing to Defendant's current and former customers and  
 22 applicants that it did not follow industry best practices for the collection, use, and  
 23 storage of Private Information.

24 357. As a direct and proximate result of the unconscionable, unfair, and  
 25 deceptive acts or practices alleged herein, Plaintiff and Class Members are entitled  
 26 to recover an order providing declaratory relief and reasonable attorneys' fees and  
 27 costs, to the extent permitted by law.  
 28

358. Also, as a direct result of Defendant's knowing violation of the Florida Unfair and Deceptive Trade Practices Act, Plaintiffs and Class Members are entitled to injunctive relief, including, but not limited to:

- ordering that Defendant implement measures that ensure that the Private Information of Defendant's current and former customers and applicants is appropriately encrypted and safeguarded when stored on Defendant's network or systems;
- ordering that Defendant purge, delete, and destroy in a reasonable secure manner Private Information not necessary for its provision of services;
- ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and
- ordering Defendant to meaningfully educate its current and former customers and applicants about the threats they face as a result of the accessibility of their Private Information to third parties, as well as the steps Defendant's current and former customers must take to protect themselves.

**TENTH CAUSE OF ACTION**  
**Violations of the New York Deceptive Trade Practices Act**  
**New York Gen. Bus. Law § 349**  
**(On Behalf of Plaintiffs Hernandez and Ricco-Brown and the New York Subclass Against Defendant)**

359. Plaintiffs Hernandez and Ricco-Brown ("Plaintiffs" for the purposes of this count) re-alleges and incorporates by reference all other paragraphs of this complaint as though fully set forth herein and brings this claim on behalf of himself and the New York Subclass (the "Class" for the purposes of this count).

360. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and furnishing of services, in violation of N.Y. Gen. Bus. Law § 349(a), including but not limited to the following:

- misrepresenting material facts to Plaintiff and the Class by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Class Members'



1 Private Information from unauthorized disclosure, release, data  
2 breaches, and theft;

- 3 • misrepresenting material facts to Plaintiffs and the Class by  
4 representing that it did and would comply with the requirements  
5 of federal and state laws pertaining to the privacy and security of  
6 Class Members' Private Information;
- 7 • omitting, suppressing, and/or concealing material facts of the  
8 inadequacy of its privacy and security protections for Class  
9 Members' Private Information;
- 10 • engaging in deceptive, unfair, and unlawful trade acts or practices  
11 by failing to maintain the privacy and security of Class Members'  
12 Private Information, in violation of duties imposed by and public  
13 policies reflected in applicable federal and state laws; and
- 14 • engaging in deceptive, unfair, and unlawful trade acts or practices  
15 by failing to disclose the Data Breach to the Class in a timely and  
16 accurate manner, contrary to the duties imposed by N.Y. Gen. Bus.  
17 Law § 899-aa (2).

18 361. Defendant knew or should have known that its network and data security  
19 practices were inadequate to safeguard Plaintiffs' and the Class Members' Private  
20 Information entrusted to it, and that the risk of a data breach or theft was highly likely.

21 362. Defendant should have disclosed this information because Defendant  
22 was in a superior position to know the true facts related to the defective data security.

23 363. Defendant's failure constitutes false and misleading representations,  
24 which have the capacity, tendency, and effect of deceiving or misleading consumers  
25 (including Plaintiffs and Class Members) regarding the security of Defendant's  
26 network and aggregation of Private Information.

27 364. The representations upon which consumers (including Plaintiffs and  
28 Class Members) relied were material representations (e.g., as to Defendant's  
adequate protection of Private Information), and consumers (including Plaintiffs and  
Class Members) relied on those representations to their detriment.

//

1           365. Defendant's conduct is unconscionable, deceptive, and unfair, as it is  
2 likely to, and did, mislead consumers acting reasonably under the circumstances. As  
3 a direct and proximate result of Defendant's conduct, Plaintiffs and other Class  
4 Members have been harmed, in that they were not timely notified of the Data Breach,  
5 which resulted in profound vulnerability to their personal information and other  
6 financial accounts.

7           366. Defendant knew or should have known that its computer systems and  
8 data security practices were inadequate to safeguard Class Members' Private  
9 Information and that the risk of a data security incident was high.

10           367. Defendant's acts, practices, and omissions were done in the course of  
11 Defendant's business of furnishing employment benefit services to consumers in the  
12 State of New York.

13           368. As a direct and proximate result of Defendant's unconscionable, unfair,  
14 and deceptive acts and omissions, Plaintiffs' and Class Members' Private  
15 Information was disclosed to third parties without authorization, causing and will  
16 continue to cause Plaintiffs and Class Members damages.

17           369. As a direct and proximate result of Defendant's multiple, separate  
18 violations of GBL §349, Plaintiffs and Class Members have suffered actual, concrete,  
19 and imminent injuries. The injuries suffered by Plaintiffs and the Class Members  
20 include: (a) the invasion of privacy; (b) the compromise, disclosure, theft, and  
21 unauthorized use of Plaintiffs' and Class Members' Private Information; (c)  
22 economic costs associated with the time spent to detect and prevent identity theft,  
23 including loss of productivity; (d) monetary costs associated with the detection and  
24 prevention of identity theft; (e) economic costs, including time and money, related to  
25 incidents of actual identity theft; (f) the emotional distress, fear, anxiety, nuisance  
26 and annoyance of dealing related to the theft and compromise of their Private  
27 Information; (g) the diminution in the value of the services bargained for as Plaintiffs  
28 and Class Members were deprived of the data protection and security that Defendant

1 promised when Plaintiffs and the proposed Class entrusted Defendant with their  
2 Private Information; and (h) the continued and substantial risk to Plaintiffs' and Class  
3 Members' Private Information, which remains in the Defendant's possession with  
4 inadequate measures to protect Plaintiffs' and Class Members' Private Information.

5 370. As a result, Plaintiffs and the Class Members have been damaged in an  
6 amount to be proven at trial.

7 **ELEVENTH CAUSE OF ACTION**  
8 **Violations of the Illinois Consumer Fraud and Deceptive Business Practices Act**  
9 **815 Ill. Comp. Stat. § 505/1, *et seq.***  
**(On Behalf of Plaintiff Debra Coe and Matthew McFall and the Illinois**  
**Subclass Against Defendant)**

10 371. Plaintiff Debra Coe and Matthew McFall ("Plaintiffs" for the purposes  
11 of this count) re-allege and incorporate by reference all other paragraphs of this  
12 complaint as though fully set forth herein and bring this claim on behalf of  
13 themselves and the Illinois Subclass (the "Class" for the purposes of this count).

14 372. Plaintiffs and the Class are "consumers" as defined in 815 Ill. Comp.  
15 Stat. § 505/1(e). Plaintiff, the Class, and Defendant are "persons" as defined in 815  
16 Ill. Comp. Stat. § 505/1(c).

17 373. Defendant engaged in "trade" or "commerce," including the provision of  
18 services, as defined under 815 Ill. Comp. Stat. § 505/1(f). Defendant engages in the  
19 sale of "merchandise" (including services) as defined by 815 Ill. Comp. Stat. §  
20 505/1(b) and (d).

21 374. Plaintiffs may bring claims under the ICFA because there is a consumer  
22 nexus" between Plaintiff and consumers with respect to Defendant's unfair and  
23 deceptive trade practices.

24 375. Plaintiffs' actions were akin to a consumer's action because she  
25 justifiably relied on Defendant's public statements and omissions regarding its data  
26 security practices. Specifically, Defendant's statements, including its privacy policy,  
27 states Defendant will use reasonable security measures to protect its network from  
28 cybercriminals and ransomware attacks.

1        376. Defendant's representations and omissions as to its data security  
2 measures, and its failure to implement and maintain reasonable data security  
3 measures, concern all individuals because a reasonable consumer, akin to Plaintiffs,  
4 does or is reasonably likely to rely on these statements in providing their Private  
5 Information.

6        377. Defendant's conduct involved consumer protection concerns because  
7 Defendant represented to consumers and employees (current and former) that it  
8 employed proper data security measures but, in fact, did not. Defendant's conduct  
9 also involves consumer protection concerns because Defendant's failure to  
10 implement and maintain reasonable data security measures enabled third parties to  
11 access and exfiltrate the Private Information of consumers from its network. In turn,  
12 Plaintiffs' and Class Members' Private Information is now on the dark web.

13        378. Defendant engaged in deceptive and unfair acts and practices,  
14 misrepresentation, and the concealment and omission of material facts in connection  
15 with the sale and advertisement of their services in violation of the CFA, including:  
16 (i) failing to maintain adequate data security to keep Plaintiffs' and the Class  
17 Members' sensitive Private Information from being stolen by cybercriminals and  
18 failing to comply with applicable state and federal laws and industry standards  
19 pertaining to data security, including the FTC Act; (ii) failing to disclose or omitting  
20 materials facts to Plaintiffs and the Class regarding their lack of adequate data  
21 security and inability or unwillingness to properly secure and protect the Private  
22 Information of Plaintiffs and the Class; (iii) failing to disclose or omitting materials  
23 facts to Plaintiffs and the Class about Defendant's failure to comply with the  
24 requirements of relevant federal and state laws pertaining to the privacy and security  
25 of the Private Information of Plaintiffs and the Class; and (iv) failing to take proper  
26 action following the Data Breach to enact adequate privacy and security measures  
27 and protect Plaintiffs' and the Class's Private Information and other personal  
28 information from further unauthorized disclosure, release, data breaches, and theft.

1        379. These actions also constitute deceptive and unfair acts or practices  
2 because Defendant knew the facts about its inadequate data security and failure to  
3 comply with applicable state and federal laws and industry standards would be  
4 unknown to and not easily discoverable by Plaintiffs and the Class and defeat their  
5 reasonable expectations about the security of their Private Information.

6        380. Defendant intended that Plaintiffs and the Class rely on its deceptive and  
7 unfair acts and practices and the concealment and omission of material facts in  
8 connection with Defendant's offering of goods and services.

9        381. Defendant's wrongful practices were and are injurious to the public  
10 because those practices were part of Defendant's generalized course of conduct that  
11 applied to the Class. Plaintiffs and the Class have been adversely affected by  
12 Defendant's conduct and the public was and is at risk as a result thereof.

13        382. As a result of Defendant's wrongful conduct, Plaintiffs and the Class  
14 were injured in that they never would have provided their Private Information to  
15 Defendant, or purchased Defendant's services, had they known or been told that  
16 Defendant failed to maintain sufficient security to keep their Private Information  
17 from being hacked and taken and misused by others.

18        383. As a direct and proximate result of Defendant's violations of the CFA,  
19 Plaintiffs and the Class have suffered harm as set forth in detail above.

20        384. The requested relief by Plaintiffs will assist consumers because it will  
21 require Defendant to enhance its data security practices. Specifically, the Complaint  
22 seeks injunctive relief, etc. Moreover, any monetary compensation will deter  
23 Defendant from additional and future data breach incidents.

24                                    **TWELFTH CAUSE OF ACTION**  
25                                    **Violation of the Arizona Consumer Fraud Act,**  
26                                    **Ariz. Rev. Stat. § 44-1521, *et seq.***  
                                  **(On Behalf of Plaintiff Ware and the Arizona Subclass)**

27        385. Plaintiffs re-alleges and incorporates by reference all other paragraphs of  
28 this complaint as though fully set forth herein and bring this claim on behalf of

1 themselves and the Nationwide Class, or, alternatively, Plaintiff Ware and the  
2 Arizona Subclass.

3 386. The ACFA provides that “[t]he act, use or employment by any person of  
4 any deception, deceptive or unfair act or practice, fraud, false pretense, false promise,  
5 misrepresentation, or concealment, suppression or omission of any material fact with  
6 intent that others rely on such concealment, suppression or omission, in connection  
7 with the sale or advertisement of any merchandise whether or not any person has in  
8 fact been misled, deceived or damaged thereby, is declared to be an unlawful  
9 practice.” Ariz. Rev. Stat. § 44-1522.

10 387. Defendant is a person as defined by Ariz. Rev. Stat. § 44-1521(6).

11 388. Defendant advertised, offered, or sold goods or services in Arizona and  
12 engaged in trade or commerce directly or indirectly affecting the people of Arizona.

13 389. Defendant engaged in deceptive and unfair acts and practices,  
14 misrepresentation, and the concealment, suppression, and omission of material facts  
15 affecting the people of Arizona in connection with the sale and advertisement of  
16 “merchandise” (as defined in Arizona Consumer Fraud Act, Ariz. Rev. Stat. § 44-  
17 1521(5)) in violation of Ariz. Rev. Stat. § 44-1522(A), including, but not limited to,  
18 the following:

- 19 a. Failing to implement and maintain reasonable security  
20 and privacy measures to protect Plaintiffs and Class  
21 Members’ Private Information, which was a direct and  
22 proximate cause of the Data Breach;
- 23 b. Failing to identify foreseeable security and privacy risks,  
24 remediate identified security and privacy risks, and  
25 adequately improve security and privacy measures  
26 following previous cybersecurity incidents, which was a  
27 direct and proximate cause of the Data Breach;
- 28 c. Failing to comply with common law and statutory duties

1                   pertaining to the security and privacy of Plaintiffs and  
2                   Class Members' Private Information, including duties  
3                   imposed by the FTC Act, 15 U.S.C. § 45, which was a  
4                   direct and proximate cause of the Data Breach;

5                   d.   Misrepresenting that it would protect the privacy and  
6                   confidentiality of Plaintiffs and Class Members' Private  
7                   Information, including by implementing and maintaining  
8                   reasonable security measures;

9                   e.   Misrepresenting that it would comply with common law  
10                  and statutory duties pertaining to the security and privacy  
11                  of Plaintiffs and Class Members' Private Information,  
12                  including duties imposed by the FTC Act, 15 U.S.C. §  
13                  45;

14                  f.   Omitting, suppressing, and concealing the material fact  
15                  that it did not reasonably or adequately secure Plaintiffs  
16                  and Class Members' Private Information; and

17                  g.   Omitting, suppressing, and concealing the material fact  
18                  that it did not comply with common law and statutory  
19                  duties pertaining to the security and privacy of Plaintiffs  
20                  and Class Members' Private Information, including  
21                  duties imposed by the FTC Act, 15 U.S.C. § 45.

22           390. Defendant's representations and omissions were material because they  
23           were likely to deceive reasonable consumers about the adequacy of Defendant's data  
24           security and ability to protect the confidentiality of consumers' Private Information.

25           391. Defendant intended to, and did, mislead Plaintiffs and Class Members  
26           and induced them to rely on its misrepresentations and omissions.

27           392. Had Defendant disclosed to Plaintiffs and Class Members that its data  
28           systems were not secure and, thus, vulnerable to attack, Defendant would have been  
          unable to continue in business and it would have been forced to adopt reasonable



1 data security measures and comply with the law. Instead, Defendant received,  
2 maintained, and compiled Plaintiffs' and Class Members' Private Information as part  
3 of the services Defendant provided and for which Plaintiffs and Class Members paid  
4 without advising Plaintiffs and Class Members that Defendant's data security  
5 practices were insufficient to maintain the safety and confidentiality of Plaintiffs'  
6 and Class Members' Private Information. Accordingly, Plaintiffs and the Class  
7 Members acted reasonably in relying on Defendant's misrepresentations and  
8 omissions, the truth of which they could not have discovered.

9 393. Defendant acted intentionally, knowingly, and maliciously to violate  
10 Arizona's Consumer Fraud Act, and recklessly disregarded Plaintiffs and Class  
11 Members' rights. Defendant were on notice that their security and privacy protections  
12 were inadequate and that they were targets of such attacks.

13 394. As a direct and proximate result of Defendant's unfair and deceptive acts  
14 and practices, Plaintiffs and Class Members have suffered and will continue to suffer  
15 injury, ascertainable losses of money or property, and monetary and non-monetary  
16 damages, including from fraud and identity theft; time and expenses related to  
17 monitoring their financial accounts for fraudulent activity and cancelling and  
18 replacing passports; an increased, imminent risk of fraud and identity theft; and loss  
19 of value of their Private Information.

20 395. Plaintiffs and Class Members seek all monetary and non-monetary relief  
21 allowed by law, including compensatory damages; disgorgement; punitive damages;  
22 injunctive relief; and reasonable attorneys' fees and costs.

23  
24 **THIRTEENTH CAUSE OF ACTION**  
25 **Violation of the Colorado Consumer Protection Act**  
**Colo. Rev. Stat. § 6-1-101, *et seq.***  
**(On Behalf of Plaintiff Beller and the Colorado Subclass)**

26 396. Plaintiffs re-allege and incorporate by reference all other paragraphs of  
27 this complaint as though fully set forth herein and bring this claim on behalf of  
28 themselves and the Nationwide Class, or, alternatively, Plaintiff Beller and the

1 Colorado Subclass.

2 397. Defendant engaged in unlawful, unfair, and deceptive acts and practices,  
3 with respect to the sale and advertisement of services paid for by Plaintiffs and the  
4 Class Members in violation of Colo. Rev. Stat. § 6-1-105, including by representing  
5 that Defendant would safeguard Plaintiffs and the Class Members' Private  
6 Information from unauthorized disclosure and release, and comply with relevant state  
7 and federal privacy laws, including the following:

- 8 a. Failing to implement and maintain reasonable security  
9 and privacy measures to protect Plaintiffs and Class  
10 Members' Private Information, which was a direct and  
11 proximate cause of the Data Breach;
- 12 b. Failing to identify foreseeable security and privacy risks,  
13 remediate identified security and privacy risks, and  
14 adequately improve security and privacy measures  
15 following previous cybersecurity incidents, which was a  
16 direct and proximate cause of the Data Breach;
- 17 c. Failing to comply with common law and statutory duties  
18 pertaining to the security and privacy of Plaintiffs and  
19 Class Members' Private Information, including duties  
20 imposed by the FTC Act, 15 U.S.C. § 45, which was a  
21 direct and proximate cause of the Data Breach;
- 22 d. Misrepresenting that it would protect the privacy and  
23 confidentiality of Plaintiffs and Class Members' Private  
24 Information, including by implementing and maintaining  
25 reasonable security measures;
- 26 e. Misrepresenting that it would comply with common law  
27 and statutory duties pertaining to the security and privacy  
28 of Plaintiffs and Class Members' Private Information,  
including duties imposed by the FTC Act, 15 U.S.C. §

45;

- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs and Class Members' Private Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

398. Defendant's inadequate data security had no countervailing benefit to consumers or to competition. Defendant intended to mislead Plaintiffs and Class Members and induce them to rely on its misrepresentations and omissions. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of the Defendant's data security and ability to protect the confidentiality of consumers' Private Information.

399. The above unfair and deceptive practices and acts by Defendant were immoral, unethical, oppressive, and unscrupulous.

400. Defendant knew or should have known that its network and data security practices were inadequate to safeguard Plaintiffs' and the Class Members' Private Information entrusted to it, and that the risk of a data breach or theft was highly likely.

401. Defendant's actions were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiffs and the Class Members.

402. As a direct and proximate result of Defendant's deceptive acts and practices, Plaintiffs and the Class Members suffered an ascertainable loss of money or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their Private Information.

403. Plaintiffs and the Class Members seek relief under Colo. Rev. Stat. § 6-1-101 including, but not limited to injunctive relief, compensatory damages,

1 restitution, statutory damages, penalties, and attorneys' fees and costs.

2 **FOURTEENTH CAUSE OF ACTION**  
3 **Violation of the Maine Uniform Deceptive Trade Practices Act**  
4 **10 Me. Rev. Stat. § 1212, *et seq.***  
5 **(On Behalf of Plaintiff McPhail and the Maine Subclass)**

6 404. Plaintiffs re-allege and incorporate by reference all other paragraphs of  
7 this complaint as though fully set forth herein and bring this claim on behalf of  
8 themselves and the Nationwide Class, or, alternatively, Plaintiff McPhail and the  
9 Maine Subclass.

10 405. Defendant engaged in unlawful, unfair, and deceptive acts and  
11 practices, with respect to the sale and advertisement of the services paid for by  
12 Plaintiffs and the Class members, in violation of 5 Me. Rev. Stat. § 1212(E), (G),  
13 including by representing that Defendant would adequately protect Plaintiffs' and the  
14 Class members' Private Information from unauthorized disclosure and release, and  
15 comply with relevant state and federal privacy laws, including the following:

- 16 a. Failing to implement and maintain reasonable security  
17 and privacy measures to protect Plaintiffs and Class  
18 Members' Private Information, which was a direct and  
19 proximate cause of the Data Breach;
- 20 b. Failing to identify foreseeable security and privacy risks,  
21 remediate identified security and privacy risks, and  
22 adequately improve security and privacy measures  
23 following previous cybersecurity incidents, which was a  
24 direct and proximate cause of the Data Breach;
- 25 c. Failing to comply with common law and statutory duties  
26 pertaining to the security and privacy of Plaintiffs and  
27 Class Members' Private Information, including duties  
28 imposed by the FTC Act, 15 U.S.C. § 45, which was a  
direct and proximate cause of the Data Breach;

- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs and Class Members' Private Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs and Class Members' Private Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

406. Defendant's inadequate data security had no countervailing benefit to consumers or to competition. Defendant intended to mislead Plaintiffs and Class Members and induce them to rely on its misrepresentations and omissions. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of the Defendant's data security and ability to protect the confidentiality of consumers' Private Information.

407. The above unfair and deceptive practices and acts by Defendant were immoral, unethical, oppressive, and unscrupulous.

408. Defendant knew or should have known that its network and data security practices were inadequate to safeguard Plaintiffs' and the Class Members' Private Information entrusted to it, and that the risk of a data breach or theft was highly likely.

1           409. Defendant's actions were negligent, knowing and willful, and/or wanton  
2 and reckless with respect to the rights of Plaintiffs and the Class Members.

3           410. As a direct and proximate result of Defendant's deceptive acts and  
4 practices, Plaintiffs and the Class Members suffered an ascertainable loss of money  
5 or property, real or personal, as described above, including the loss of their legally  
6 protected interest in the confidentiality and privacy of their Private Information.

7           411. Plaintiffs and the Class Members seek relief under 5 Me. Rev. Stat. §  
8 1213, including but not limited to injunctive relief and attorneys' fees and costs.

9                                   **FIFTEENTH CAUSE OF ACTION**  
10                               **Violation of the North Carolina Unfair Trade Practices Act**  
11                               **N.C. Gen. Stat. An. § 75-1.1, *et seq.***  
12                               **(On Behalf of Plaintiff Beckwith and the North Carolina Subclass)**

13           412. Plaintiffs re-allege and incorporate by reference all other paragraphs of  
14 this complaint as though fully set forth herein and bring this claim on behalf of  
15 themselves and the Nationwide Class, or, alternatively, Plaintiff Beckwith and the  
16 North Carolina Subclass.

17           413. Defendant's sale, advertising, and marketing of home loan services  
18 affected commerce, as meant by N.C. Gen. Stat. § 75-1.1.

19           414. Defendant engaged in unlawful, unfair, and deceptive acts and  
20 practices, with respect to the sale and advertisement of the services paid for by  
21 Plaintiffs and the Class members, in violation of N.C. Gen. Stat. § 75-1.1, including  
22 by representing that Defendant would adequately protect Plaintiffs' and the Class  
23 members' Private Information from unauthorized disclosure and release, and comply  
24 with relevant state and federal privacy laws, including the following:

- 25                   a. Failing to implement and maintain reasonable security  
26                   and privacy measures to protect Plaintiffs and Class  
27                   Members' Private Information, which was a direct and  
28                   proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks,

1 remediate identified security and privacy risks, and  
2 adequately improve security and privacy measures  
3 following previous cybersecurity incidents, which was a  
4 direct and proximate cause of the Data Breach;

5 c. Failing to comply with common law and statutory duties  
6 pertaining to the security and privacy of Plaintiffs and  
7 Class Members' Private Information, including duties  
8 imposed by the FTC Act, 15 U.S.C. § 45, which was a  
9 direct and proximate cause of the Data Breach;

10 d. Misrepresenting that it would protect the privacy and  
11 confidentiality of Plaintiffs and Class Members' Private  
12 Information, including by implementing and maintaining  
13 reasonable security measures;

14 e. Misrepresenting that it would comply with common law  
15 and statutory duties pertaining to the security and privacy  
16 of Plaintiffs and Class Members' Private Information,  
17 including duties imposed by the FTC Act, 15 U.S.C. §  
18 45;

19 f. Omitting, suppressing, and concealing the material fact  
20 that it did not reasonably or adequately secure Plaintiffs  
21 and Class Members' Private Information; and

22 g. Omitting, suppressing, and concealing the material fact  
23 that it did not comply with common law and statutory  
24 duties pertaining to the security and privacy of Plaintiffs  
25 and Class Members' Private Information, including  
26 duties imposed by the FTC Act, 15 U.S.C. § 45.

27 415. Defendant's inadequate data security had no countervailing benefit to  
28 consumers or to competition. Defendant intended to mislead Plaintiffs and Class  
Members and induce them to rely on its misrepresentations and omissions.



1 Defendant's representations and omissions were material because they were likely to  
2 deceive reasonable consumers about the adequacy of the Defendant's data security  
3 and ability to protect the confidentiality of consumers' Private Information.

4 416. The above unfair and deceptive practices and acts by Defendant were  
5 immoral, unethical, oppressive, and unscrupulous.

6 417. Defendant knew or should have known that its network and data security  
7 practices were inadequate to safeguard Plaintiffs' and the Class Members' Private  
8 Information entrusted to it, and that the risk of a data breach or theft was highly likely.

9 418. Defendant's actions were negligent, knowing and willful, and/or wanton  
10 and reckless with respect to the rights of Plaintiffs and the Class Members.

11 419. As a direct and proximate result of Defendant's deceptive acts and  
12 practices, Plaintiffs and the Class Members suffered an ascertainable loss of money  
13 or property, real or personal, as described above, including the loss of their legally  
14 protected interest in the confidentiality and privacy of their Private Information.

15 420. Plaintiffs and the Class Members seek relief under N.C. Gen. Stat. Ann.  
16 §§ 75-16 and 75-16.1, including, but not limited to injunctive relief, actual damages,  
17 treble damages, and attorneys' fees and costs.

18 **SIXTEENTH CAUSE OF ACTION**  
19 **Declaratory and Injunctive Relief**  
**(On Behalf of Plaintiffs and the Nationwide Class Against Defendant)**

20 421. Plaintiffs re-allege and incorporate by reference all other paragraphs of  
21 this complaint as though fully set forth herein.

22 422. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this  
23 Court is authorized to enter a judgment declaring the rights and legal relations of the  
24 parties and grant further necessary relief. Furthermore, the Court has broad authority  
25 to restrain acts, such as those alleged herein, which are tortious and which violate the  
26 terms of the federal and state statutes described above.

27 423. An actual controversy has arisen in the wake of the Data Breach at issue  
28 regarding Defendant's common law and other duties to act reasonably with respect to

1 safeguarding the data of Plaintiffs and the Class. Plaintiffs allege Defendant's actions  
2 in this respect were inadequate and unreasonable and, upon information and belief,  
3 remain inadequate and unreasonable. Additionally, Plaintiffs and the Class continue  
4 to suffer injury due to the continued and ongoing threat of additional fraud against  
5 them or on their accounts.

6 424. Under its authority under the Declaratory Judgment Act, this Court  
7 should enter a judgment declaring, among other things, the following:

8 425. Defendant owed, and continues to owe, a legal duty to employ  
9 reasonable data security to secure the Private Information it possesses, and to notify  
10 impacted individuals of the Data Breach under the common law and Section 5 of the  
11 FTC Act;

12 426. Defendant breached, and continues to breach, its duty by failing to  
13 employ reasonable measures to secure its customers' personal and financial  
14 information; and

15 427. Defendant's breach of its legal duty continues to cause harm to Plaintiffs  
16 and the Class.

17 428. The Court should also issue corresponding injunctive relief requiring  
18 Defendant to employ adequate security protocols consistent with industry standards  
19 to protect its customers' (i.e., Plaintiffs and Class Members') data.

20 429. If an injunction is not issued, Plaintiffs and the Class will suffer  
21 irreparable injury and lack an adequate legal remedy in the event of another breach of  
22 Defendant's data systems. If another breach of Defendant's data systems occurs,  
23 Plaintiffs and the Class will not have an adequate remedy at law because many of the  
24 resulting injuries are not readily quantified in full, and they will be forced to bring  
25 multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while  
26 warranted to compensate Plaintiffs and the Class for their out-of-pocket and other  
27 damages that are legally quantifiable and provable, do not cover the full extent of  
28 injuries suffered by Plaintiffs and the Class, which include monetary damages that are

1 not legally quantifiable or provable.

2 430. An injunction would benefit the public by preventing another data  
3 breach, thus eliminating the injuries that would result to Plaintiff, the Class, and the  
4 public at large.

5 **IX. REQUEST FOR RELIEF**

6 WHEREFORE, Plaintiffs, on behalf of themselves and the Class set forth  
7 herein, respectfully request the following relief:

- 8 1. For an Order certifying the proposed Class and any appropriate  
9 Subclasses, pursuant to California Civil Code Section 382, requiring  
10 notice thereto to be paid by Defendant and appointing Plaintiffs and their  
11 counsel to represent the Class(es);
- 12 2. For appropriate injunctive relief and/or declaratory relief, including, but  
13 not limited to, an order requiring Defendant to immediately secure and  
14 fully encrypt all confidential information, to store any computer  
15 passwords in a location separate from the computers, to cease negligently  
16 storing, handling, and securing their customers' confidential  
17 information, to notify customers whose Private Information was wrongly  
18 disclosed in an expedient and timely manner and to provide identity theft  
19 monitoring for an additional five years;
- 20 3. Adjudging and decreeing that Defendant has engaged in the conduct  
21 alleged herein;
- 22 4. For compensatory and general damages according to proof of certain  
23 causes of action;
- 24 5. For statutory damages on certain causes of action, including, but not  
25 limited to, statutory damages under the CCPA in an amount not less than  
26 one hundred dollars (\$100) and not greater than seven hundred and fifty  
27 (\$750) per consumer per incident or actual damages, whichever is  
28 greater, and all other damages available by statute or law;

6. For reimbursement, restitution and disgorgement on certain causes of action;
7. For both pre and post-judgment interest at the maximum allowable rate on any amounts awarded;
8. For costs of the proceedings herein;
9. For reasonable attorneys' fees, as allowed by statute; and
10. For any and all such other and further relief that this Court may deem just and proper, including, but not limited to, punitive or exemplary damages.

Dated: June 3, 2024

/s/ Daniel S. Robinson

Daniel S. Robinson  
ROBINSON CALCAGNIE, INC.  
19 Corporate Plaza Drive  
Newport Beach, California  
(949) 720-1288; Fax: (949) 720-1292  
drobinson@robinsonfirm.com

/s/ Tina Wolfson

Tina Wolfson  
AHDoot & Wolfson, PC  
2600 W Olive Ave, Ste 500  
Burbank, California 91505  
(310) 474-9111; Fax: (310) 474-8585  
twolfson@ahdootwolfson.com

/s/ Abbas Kazerounian

Abbas Kazerounian  
KAZEROUNI LAW GROUP, APC  
245 Fischer Avenue, Suite D1  
Costa Mesa, California 92626  
(800) 400-6808; Fax: (800) 520-5523  
ak@kazlg.com

/s/ Stephen G. Larson

Stephen G. Larson  
LARSON, LLP  
555 S. Flower Street, 30th Floor  
Los Angeles, CA 90071  
(213) 436-4864; Fax: (213) 623-2000  
slarson@larsonllp.com

/s/ Gary M. Klinger

Gary M. Klinger  
MILBERG COLEMAN BRYSON  
PHILLIPS GROSSMAN, PLLC  
227 W. Monroe Street, Suite 2100  
Chicago, IL 60606  
(866) 252-0878

***Interim Co-Lead Counsel for Plaintiffs***

**DEMAND FOR JURY TRIAL**

Plaintiffs hereby demand a trial by jury on all issues in this action so triable of right.

Dated: June 3, 2024

/s/ Daniel S. Robinson

Daniel S. Robinson  
ROBINSON CALCAGNIE, INC.  
19 Corporate Plaza Drive  
Newport Beach, California  
(949) 720-1288; Fax: (949) 720-1292  
drobinson@robinsonfirm.com

/s/ Stephen G. Larson

Stephen G. Larson  
LARSON, LLP  
555 S. Flower Street, 30th Floor  
Los Angeles, CA 90071  
(213) 436-4864; Fax: (213) 623-2000  
slarson@larsonllp.com

/s/ Tina Wolfson

Tina Wolfson  
AHDoot & Wolfson, PC  
2600 W Olive Ave, Ste 500  
Burbank, California 91505  
(310) 474-9111; Fax: (310) 474-8585  
twolfson@ahdootwolfson.com

/s/ Gary M. Klinger

Gary M. Klinger  
MILBERG COLEMAN BRYSON  
PHILLIPS GROSSMAN, PLLC  
227 W. Monroe Street, Suite 2100  
Chicago, IL 60606  
(866) 252-0878

/s/ Abbas Kazerounian

Abbas Kazerounian  
KAZEROUNI LAW GROUP, APC  
245 Fischer Avenue, Suite D1  
Costa Mesa, California 92626  
(800) 400-6808; Fax: (800) 520-5523  
ak@kazlg.com

***Interim Co-Lead Counsel for Plaintiffs***